PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-085321

(43)Date of publication of application : 20.03.2003

---

(51)Int.Cl. G06F 17/60
H04L 9/08
H04N 7/167

---

(21)Application number : 2001-274854 (71)Applicant : SONY CORP

(22)Date of filing : 11.09.2001 (72)Inventor : OKA MAKOTO
ISHIBASHI YOSHITO
ABE HIROSHI
SHIMADA NOBORU
ENARI MASAHIKO
YOSHINO KENJI

---

(54) SYSTEM AND METHOD FOR CONTENTS USE AUTHORITY CONTROL, INFORMATION PROCESSING DEVICE, AND COMPUTER PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a system capable of upgrading contents use conditions by eliminating the need of the contents use authority control by users on a service provider side.

SOLUTION: In this system, enciphered contents are distributed, and the use of the contents is allowed by only formal users. A service provider receives a contents use

authority certificate from the users, acquires the user information and the contents purchase information of the users from the contents use authority certificate on conditions that it is confirmed by the verification of the electronic signature of the issue entity of the contents use authority certificate that data is not tampered, and the upgrade processing of use condition alteration is performed. Thus a contents use condition alteration processing can be performed even if the service provider side does not have user control data.

LEGAL STATUS [Date of request for examination] 19.02.2003
[Date of sending the examiner's decision of rejection] 15.11.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It has a user device using contents, and the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device. While said user device has the configuration which performs contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider Said contents use authority certificate is sent to said service provider. It has the configuration which performs a modification processing demand of the contents use condition information stored in the contents use authority certificate. Said service provider It responds to reception of said contents use authority certificate accompanied by a modification processing demand of the contents use condition information from said user device. The contents use authority administration system characterized by having the configuration which performs processing which generates the upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate, and is transmitted to a user device.
[Claim 2] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said user device It is contingent [on the judgment of being contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider]. The contents use authority administration system according to claim 1 characterized by being the configuration which performs decode of said encryption contents key and acquires a contents key.
[Claim 3] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said user device On the occasion of contents use, judgment processing of whether to be contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. The contents use

authority administration system according to claim 1 characterized by having the configuration which performs decryption processing of the encryption contents key stored in said contents use authority certificate based on the key stored in the user device.

[Claim 4] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said service provider On the occasion of the contents use in a user device, a sent contents use authority certificate is received from this user device. Judgment processing of whether to be contents use according to the contents use condition information stored in the received contents use authority certificate is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. The contents use authority administration system according to claim 1 characterized by having the configuration which performs decryption processing of the encryption contents key stored in said contents use authority certificate based on a service provider proper key.

[Claim 5] The contents use condition information stored in said contents use authority certificate Contents buying up which does not prepare contents use time limitation information, the count limit information of contents use, and a use limit is either [like] 3 voice. A modification processing demand of the use condition information on the contents from said user device Modification of contents use time limitation, or modification of the count limit of contents use, Either is included even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up, perform either and an upgrade contents use authority certificate is generated. The contents use authority administration system according to claim 1 characterized by having the configuration which performs processing transmitted to a user device.

[Claim 6] The online use processing which makes an indispensable condition use authority judging processing in a service provider at the contents use conditions stored in said contents use authority certificate, The use condition information that

either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate The contents use authority administration system according to claim 1 characterized by having the configuration which performs use condition change information between online use processing and off-line use processing, and performs processing which generates an upgrade contents use authority certificate and is transmitted to a user device.

[Claim 7] Said contents use authority certificate is a contents use authority administration system according to claim 1 characterized by being the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider being the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[Claim 8] Said contents use authority certificate is the contents use authority-administration system according to claim 1 which is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate, and is characterized by to be the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate with which said service provider is acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.

[Claim 9] Said contents use authority certificate is a contents use authority administration system according to claim 1 characterized by being the attribute certificate which an attribute certificate certificate authority publishes, and being the configuration of having stored in attribute information field attribute certification in the letter the encryption contents key which enciphered the contents key applied to decode of contents.

[Claim 10] Said contents use authority certificate is a contents use authority administration system according to claim 1 characterized by being the attribute certificate which an attribute certificate certificate authority publishes, and being the configuration of having stored the use conditions of contents in attribute information

field attribute certification in the letter.
[Claim 11] It has a user device using contents, and the service provider which distributes the contents use authority certificate which stored purchase contents information to a user device. Said user device sends said contents use authority certificate to said service provider. Said service provider It is based on the contents information stored in the contents use authority certificate received from said user device. The contents use authority certificate corresponding to the contents belonging to the same album identified as the same set contents as this contents information is generated as an upgrade contents use authority certificate. The contents use authority administration system characterized by having the configuration which performs processing transmitted to a user device.
[Claim 12] Said contents use authority certificate is a contents use authority administration system according to claim 11 characterized by being the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider being the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.
[Claim 13] Said contents use authority certificate is the contents use authority-administration system according to claim 11 which is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate, and is characterized by to be the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate with which said service provider is acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.
[Claim 14] It is the contents use authority administration approach in the system which has a user device using contents, and the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device. Said user device Said contents use authority certificate is sent to said service provider. A modification processing demand of the contents use condition information stored in the contents use authority certificate is performed. Said service provider It responds to reception of said contents use authority certificate accompanied by a modification processing demand of the contents use condition information from said user device. The contents use authority administration

approach characterized by performing processing which generates the upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate, and is transmitted to a user device.

[Claim 15] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said user device It is contingent [on the judgment of being contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider]. The contents use authority administration approach according to claim 14 characterized by performing decode of said encryption contents key and acquiring a contents key.

[Claim 16] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said user device On the occasion of contents use, judgment processing of whether to be contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. The contents use authority administration approach according to claim 14 characterized by performing decryption processing of the encryption contents key stored in said contents use authority certificate based on the key stored in the user device.

[Claim 17] The encryption contents key which enciphered Kc is stored. A contents key for said contents use authority certificate to decode encryption contents : said service provider On the occasion of the contents use in a user device, a sent contents use authority certificate is received from this user device. Judgment processing of whether to be contents use according to the contents use condition information stored in the received contents use authority certificate is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. The contents use authority administration approach according to claim 14 characterized by performing decryption processing of the encryption contents key stored in said contents use authority certificate based on a service provider proper key.

[Claim 18] The contents use condition information stored in said contents use authority certificate Contents buying up which does not prepare contents use time limitation information, the count limit information of contents use, and a use limit is either [like] 3 voice. A modification processing demand of the use condition

information on the contents from said user device Modification of contents use time limitation, or modification of the count limit of contents use, Either is included even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up, perform either and an upgrade contents use authority certificate is generated. The contents use authority administration approach according to claim 14 characterized by performing processing transmitted to a user device.

[Claim 19] The online use processing which makes an indispensable condition use authority judging processing in a service provider at the contents use conditions stored in said contents use authority certificate, The use condition information that either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate The contents use authority administration approach according to claim 14 characterized by performing use condition change information between online use processing and off-line use processing, and performing processing which generates an upgrade contents use authority certificate and is transmitted to a user device.

[Claim 20] Said contents use authority certificate is the contents use authority administration approach according to claim 14 characterized by being the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[Claim 21] Said contents use authority certificate is the contents use authority-administration approach according to claim 14 characterized by to perform the justification check of this contents use authority certificate as conditions by

verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on [are the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate, and] reception of said contents use authority certificate in said service provider.

[Claim 22] It is the contents use authority administration approach in the system which has a user device using contents, and the service provider which distributes the contents use authority certificate which stored purchase contents information to a user device. Said user device Said contents use authority certificate is sent to said service provider. Said service provider It is based on the contents information stored in the contents use authority certificate received from said user device. The contents use authority certificate corresponding to the contents belonging to the same album identified as the same set contents as this contents information is generated as an upgrade contents use authority certificate. The contents use authority administration approach characterized by performing processing transmitted to a user device.

[Claim 23] Said contents use authority certificate is the contents use authority administration approach according to claim 22 characterized by being the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[Claim 24] Said contents use authority certificate is the contents use authority-administration approach according to claim 22 characterized by ****** which performs the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on [are the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate, and] reception of said contents use authority certificate in said service provider.

[Claim 25] In the system which has a user device using contents, and the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device Are the information processor which publishes a contents use authority certificate, and the contents use condition modification processing demand accompanied by contents use condition information [finishing / issue] is received from a user device. Verification processing of the

received contents use authority certificate is performed, and it is contingent [on the justification of said contents use authority certificate having been checked by this verification]. The information processor characterized by having the configuration which performs processing which generates the upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate, and is transmitted to a user device.

[Claim 26] Said information processor responds to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device. As modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up, perform either and an upgrade contents use authority certificate is generated. The information processor according to claim 25 characterized by having the configuration which performs processing transmitted to a user device.

[Claim 27] The online use processing which makes an indispensable condition use authority judging processing in a service provider at the contents use conditions stored in said contents use authority certificate, The use condition information that either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said information processor According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate The information processor according to claim 25 characterized by having the configuration which performs use condition change information between online use processing and off-line use processing, and performs processing which generates an upgrade contents use authority certificate and is transmitted to a user device.

[Claim 28] Said contents use authority certificate is an information processor according to claim 25 characterized by being the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said information processor being the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[Claim 29] Said contents use authority certificate is the information processor according to claim 25 which is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate, and is characterized by to be the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate with which said information processor is acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.
[Claim 30] In the system which has a user device using contents, and the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device The step which is the computer program which makes issue processing of a contents use authority certificate perform on computer system, and receives the contents use condition modification processing demand accompanied by contents use condition information [finishing / issue], The step which performs verification processing of the received contents use authority certificate, It is contingent [on the justification of said contents use authority certificate having been checked by this verification]. The computer program characterized by having the step which generates the upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate, and is transmitted to a user device.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a contents use authority administration system, the contents use authority administration approach and an information processor, and a list at a computer program. By delivery of the contents key which used a contents use authority certificate including the use authority information on contents etc., for example, an attribute certificate, in the system which distributes the contents enciphered especially While preventing unjust use of contents, based on a contents use authority certificate, the contents use authority certificate corresponding to new use conditions or new contents is published. It is related with the contents use authority administration system which enabled new contents use, the contents use authority administration approach and an information processor, and a list at a computer program.

[0002]

[Description of the Prior Art] The service which distributes various software data (these are hereafter called contents (Content)), such as music data, image data, and a game program, through the various communication networks of a cable besides the communication link through the Internet and a satellite and wireless prospers these days. Moreover, the contents circulation through the storage of DVD, CD, a memory card, etc. which can be circulated also prospers. These circulation contents are set and used [reproduce and] for TV and PC (Personal Computer) which a user owns, the vessel only for playbacks, or a game device.

[0003] It is received by the set top box which has communication facility, and it is changed into refreshable data, and is reproduced, or the contents distributed through a communication network are received and reproduced by information machines and equipment, such as TV equipped with the communication interface in the regenerative apparatus besides TV, a regenerative apparatus, a game device, and PC.

[0004] Generally as for many software contents, such as a game program, music data, and image data, the right of distribution etc. is held by the implementer and the vender. Therefore, it is common to permit use of software, and for reproduction without authorization etc. to be made not to be performed, namely, to take the configuration in consideration of security only to a fixed use limit, i.e., a regular user, on the occasion of distribution of these contents.

[0005] One technique of realizing the use limit to a user is encryption processing of distribution contents. For example, when storing and distributing the contents as

which protection of copyrights is requested to media, such as distribution through satellite communication or the Internet communication link, or DVD, contents are enciphered, and it distributes or stores, and an available decode key is distributed to contents decode only to a registered user. A registered user is a configuration which performs decode of encryption contents and reproduces contents with the distributed decode key.

[0006] Encryption data can be returned to decode data (plaintext) by decryption processing which used the decode key. The data encryption and the decryption approach of using an encryption key for data encryption processing, and using a decryption key for decryption processing are well learned from the former.

[0007] Although it is seeds, there are various methods currently called the so-called common key encryptosystem-ized method as the one example in the mode of the data encryption and the decryption approach using an encryption key and a decryption key. A common key encryptosystem-ized method gives the encryption key used for data encryption processing, and the common key which uses for these encryption processing and a decryption the decryption key used for a decryption of data as a common thing at the user of normal, and eliminates the data access by the inaccurate user without a key. DES (data code criterion: Data encryption standard) is in the typical method of this method.

[0008] On the other hand, for example based on a certain password etc., a Hash Function etc. can obtain the encryption key and decryption key which are used for above-mentioned encryption processing and a decryption with the application of a tropism function. On the other hand with a tropism function, the function which becomes very difficult asks for an input conversely from the output. For example, on the other hand, a tropism function is applied by considering the password which the user decided as an input, and an encryption key and a decryption key are generated based on the output. Thus, the parenchyma top of asking for the password which is the original data conversely from the obtained encryption key and a decryption key becomes impossible.

[0009] Moreover, the method which performs processing with the encryption key used when enciphering, and processing of the decryption key used when decoding with a different key is a method called the so-called public key cryptosystem. An unspecified user is the approach of using an usable public key, and a public key cryptosystem performs encryption processing using the public key with which the specific individual generated the encryption document to a specific individual. The decryption processing of the document enciphered with the public key is attained only with the private key

corresponding to the public key used for the encryption processing. Since only the individual who generated the public key owns a private key, only an individual with a private key can decode the document enciphered with the public key. An elliptic curve cryptosystem or a RSA (Rivest-Shamir-Adleman) code is one of the typical things of a public key cryptosystem. By using such a cipher system, the system which enables the decode of encryption contents only to a registered user becomes possible.

[0010]

[Problem(s) to be Solved by the Invention] In the above contents use managerial systems, many configurations which encipher contents, store in record media, such as a network, or DVD, CD, provide for a user, and provide only a valid user with the contents key which decodes encryption contents are adopted. The contents key for preventing unjust use of the contents key itself etc. is enciphered, it provides for a valid user, and the configuration which decodes an encryption contents key using the decode key which only a valid user has, and makes a contents key usable is proposed.

[0011] The judgment of whether to be a valid user is performed by generally performing authentication processing before distribution of contents or a contents key between user devices with the content provider who is the transmitting person of contents. In general authentication processing, while checking a partner, when an effective session key is generated only by the communication link and authentication is materialized, it communicates by enciphering data, for example, contents, or a contents key using the generated session key.

[0012] However, in the configuration which performs an user validation by using such authentication processing as the base, and distributes contents or a contents key, it is necessary to manage the contents use authority information for every user by the side which distributes a contents key. That is, in order that a user may judge whether it has just contents use authority, all users' contents use authority information is stored in a database, and the processing which performs distribution of contents or a contents key is needed based on authority information.

[0013] When the number of users becomes huge, a processing load becomes large and it makes the effectiveness of distribution of contents, or the message distribution processing of a contents key fall, although it is satisfactory at all if such processing, i.e., check processing of a user's contents use authority, is the fraction of the range where the number of users using contents was restricted. Moreover, the case where he wants to change conditions set up as use conditions for contents for some users, such as time limitation and a count limit, after the purchase of contents may occur.

[0014] This invention is made in view of an above-mentioned trouble. A user's

contents use authority Contents use is enabled only in a valid user, without managing for every user by the service provider side. Furthermore, modification processing of various use limits corresponding to a user, such as time limitation and a count limit, Or it aims at providing with a computer program the contents use authority administration system which made it possible to perform the purchase of new contents based on the information corresponding to contents [finishing / purchase], the contents use authority administration approach and an information processor, and a list.

[0015]

[Means for Solving the Problem] The user device with which the 1st side face of this invention uses contents, It has the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device. Said user device While having the configuration which performs contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider Said contents use authority certificate is sent to said service provider. It has the configuration which performs a modification processing demand of the contents use condition information stored in the contents use authority certificate. Said service provider It responds to reception of said contents use authority certificate accompanied by a modification processing demand of the contents use condition information from said user device. The upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate is generated, and it is in the contents use authority administration system characterized by having the configuration which performs processing transmitted to a user device.

[0016] The contents use authority administration system of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said user device It is characterized by being the configuration which performs decode of said encryption contents key a condition [the judgment of being contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider], and acquires a contents key.

[0017] The contents use authority administration system of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said user device On the occasion of contents use,

judgment processing of whether to be contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. It is characterized by having the configuration which performs decryption processing of the encryption contents key stored in said contents use authority certificate based on the key stored in the user device.

[0018] The contents use authority administration system of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said service provider On the occasion of the contents use in a user device, a sent contents use authority certificate is received from this user device. Judgment processing of whether to be contents use according to the contents use condition information stored in the received contents use authority certificate is performed. It is contingent [on the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result]. It is characterized by having the configuration which performs decryption processing of the encryption contents key stored in said contents use authority certificate based on a service provider proper key.

[0019] Furthermore, the contents use condition information which the contents use authority administration system of this invention set like 1 operative condition, and was stored in said contents use authority certificate Contents buying up which does not prepare contents use time limitation information, the count limit information of contents use, and a use limit is either [like] 3 voice. A modification processing demand of the use condition information on the contents from said user device Modification of contents use time limitation, or modification of the count limit of contents use, Either is included even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or it is characterized by having use time limitation, the count limit of use, and the configuration that performs processing of modification between 3 modes of buying up which performs either at least, generates an upgrade contents use authority

certificate, and is transmitted to a user device.
[0020] furthermore, on the contents use conditions which the contents use authority administration system of this invention set like 1 operative condition, and were stored in said contents use authority certificate The online use processing which makes an indispensable condition use authority judging processing in a service provider, The use condition information that either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate It is characterized by having the configuration which performs use condition change information between online use processing and off-line use processing, and performs processing which generates an upgrade contents use authority certificate and is transmitted to a user device.
[0021] Furthermore, the contents use authority-administration system of this invention sets like 1 operative condition, said contents use authority certificate is the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider carries out that it is the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions as the description.
[0022] The contents use authority administration system of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate It is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate. Said service provider It is characterized by being the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.
[0023] Furthermore, the contents use authority administration system of this invention sets like 1 operative condition, and said contents use authority certificate is an attribute certificate which an attribute certificate certificate authority publishes, and is characterized by being the configuration of having stored in attribute

information field attribute certification in the letter the encryption contents key which enciphered the contents key applied to decode of contents.

[0024] Furthermore, the contents use authority administration system of this invention sets like 1 operative condition, and said contents use authority certificate is an attribute certificate which an attribute certificate certificate authority publishes, and is characterized by being the configuration of having stored the use conditions of contents in attribute information field attribute certification in the letter.

[0025] Furthermore, the user device with which the 2nd side face of this invention uses contents, It has the service provider which distributes the contents use authority certificate which stored purchase contents information to a user device. Said user device Said contents use authority certificate is sent to said service provider. Said service provider It is based on the contents information stored in the contents use authority certificate received from said user device. The contents use authority certificate corresponding to the contents belonging to the same album identified as the same set contents as this contents information is generated as an upgrade contents use authority certificate. It is in the contents use authority administration system characterized by having the configuration which performs processing transmitted to a user device.

[0026] Furthermore, the contents use authority-administration system of this invention sets like 1 operative condition, said contents use authority certificate is the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider carries out that it is the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions as the description.

[0027] The contents use authority administration system of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate It is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate. Said service provider It is characterized by being the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.

[0028] Furthermore, the user device with which the 3rd side face of this invention

uses contents, It is the contents use authority administration approach in the system which has the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device. Said user device sends said contents use authority certificate to said service provider. A modification processing demand of the contents use condition information stored in the contents use authority certificate is performed. Said service provider It responds to reception of said contents use authority certificate accompanied by a modification processing demand of the contents use condition information from said user device. The upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate is generated, and it is in the contents use authority administration approach characterized by performing processing transmitted to a user device.

[0029] The contents use authority administration approach of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said user device It is characterized by performing decode of said encryption contents key a condition [the judgment of being contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider], and acquiring a contents key.

[0030] The contents use authority administration approach of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said user device On the occasion of contents use, judgment processing of whether to be contents use according to the contents use condition information stored in the contents use authority certificate received from said service provider is performed. It is characterized by performing decryption processing of the encryption contents key stored in said contents use authority certificate based on the key stored in the user device the condition [the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result].

[0031] The contents use authority administration approach of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate The encryption contents key which enciphered Kc is stored. The contents key for decoding encryption contents : said service provider On the occasion of the contents use in a user device, a sent contents use authority certificate is received from this

user device. Judgment processing of whether to be contents use according to the contents use condition information stored in the received contents use authority certificate is performed. It is characterized by performing decryption processing of the encryption contents key stored in said contents use authority certificate based on the service provider proper key the condition [the judgment according to contents use conditions that it was contents use having been obtained based on the judgment result].

[0032] Furthermore, the contents use condition information which the contents use authority administration approach of this invention set like 1 operative condition, and was stored in said contents use authority certificate Contents buying up which does not prepare contents use time limitation information, the count limit information of contents use, and a use limit is either [like] 3 voice. A modification processing demand of the use condition information on the contents from said user device Modification of contents use time limitation, or modification of the count limit of contents use, Either is included even if there are little use time limitation, count limit of use, and modification between 3 modes of buying up. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or it is characterized by performing processing of use time limitation, the count limit of use, and modification between 3 modes of buying up which performs either at least, generates an upgrade contents use authority certificate, and is transmitted to a user device.

[0033] furthermore, on the contents use conditions which the contents use authority administration approach of this invention set like 1 operative condition, and were stored in said contents use authority certificate The online use processing which makes an indispensable condition use authority judging processing in a service provider, The use condition information that either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said service provider According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate It is characterized by performing use condition

change information between online use processing and off-line use processing, and performing processing which generates an upgrade contents use authority certificate and is transmitted to a user device.

[0034] Furthermore, the contents use authority administration approach of this invention sets like 1 operative condition, said contents use authority certificate is the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider is characterized by to perform the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[0035] The contents use authority administration approach of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate It is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate. Said service provider It is characterized by performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.

[0036] Furthermore, the user device with which the 4th side face of this invention uses contents, It is the contents use authority administration approach in the system which has the service provider which distributes the contents use authority certificate which stored purchase contents information to a user device. Said user device sends said contents use authority certificate to said service provider. Said service provider It is based on the contents information stored in the contents use authority certificate received from said user device. The contents use authority certificate corresponding to the contents belonging to the same album identified as the same set contents as this contents information is generated as an upgrade contents use authority certificate. It is in the contents use authority administration approach characterized by performing processing transmitted to a user device.

[0037] Furthermore, the contents use authority administration approach of this invention sets like 1 operative condition, said contents use authority certificate is the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said service provider is characterized by to perform the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions.

[0038] The contents use authority administration approach of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate It is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate. Said service provider It is characterized by ****** which performs the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.
[0039] Furthermore, the user device with which the 5th side face of this invention uses contents, In the system which has the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device Are the information processor which publishes a contents use authority certificate, and the contents use condition modification processing demand accompanied by contents use condition information [finishing / issue] is received from a user device. Verification processing of the received contents use authority certificate is performed, and it is contingent [on the justification of said contents use authority certificate having been checked by this verification]. The upgrade contents use authority certificate which changed the contents use condition information recorded on the received contents use authority certificate is generated, and it is in the information processor characterized by having the configuration which performs processing transmitted to a user device.
[0040] The information processor of this invention sets like 1 operative condition. Furthermore, said information processor According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate Modification of contents use time limitation, or modification of the count limit of contents use, Or it is characterized by having use time limitation, the count limit of use, and the configuration that performs processing of modification between 3 modes of buying up which performs either at least, generates an upgrade contents use authority certificate, and is transmitted to a user device.
[0041] furthermore, on the contents use conditions which the information processor of this invention set like 1 operative condition, and were stored in said contents use authority certificate The online use processing which makes an indispensable condition use authority judging processing in a service provider, The use condition

information that either of the off-line use processings which make unnecessary use authority judging processing in a service provider was set up is included. Or said information processor According to reception of said contents use authority certificate accompanied by a modification processing demand of the use condition information on the contents from said user device, as modification processing of the contents use condition information recorded on the received contents use authority certificate It is characterized by having the configuration which performs use condition change information between online use processing and off-line use processing, and performs processing which generates an upgrade contents use authority certificate and is transmitted to a user device.

[0042] Furthermore, the information processor of this invention sets like 1 operative condition, said contents use authority certificate is the configuration that the electronic signature of the issue entity of this contents use authority certificate was added, and said information processor carries out that it is the configuration of performing the check of there being no data alteration of the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate by verification of said electronic signature as conditions as the description.

[0043] The information processor of this invention sets like 1 operative condition. Furthermore, said contents use authority certificate It is the configuration of having stored the link information about the public key certificate corresponding to this contents use authority certificate. Said information processor It is characterized by being the configuration of performing the justification check of this contents use authority certificate as conditions by verification of the public key certificate acquired by said link information in the generation processing of an upgrade contents use authority certificate based on reception of said contents use authority certificate.

[0044] Furthermore, the user device with which the 6th side face of this invention uses contents, In the system which has the service provider which distributes the contents use authority certificate which stored contents use condition information to a user device The step which is the computer program which makes issue processing of a contents use authority certificate perform on computer system, and receives the contents use condition modification processing demand accompanied by contents use condition information [finishing / issue], The step which performs verification processing of the received contents use authority certificate, It is contingent [on the justification of said contents use authority certificate having been checked by this verification]. The upgrade contents use authority certificate which changed the

contents use condition information recorded on the received contents use authority certificate is generated, and it is in the computer program characterized by having the step transmitted to a user device.

[0045] In addition, the computer program of this invention is a computer program which can be offered to the computer system which can perform various program codes, for example by communication media, such as record media, such as a storage offered in a computer-readable format, communication media, for example, CD, and FD, MO, or a network. By offering such a program in a computer-readable format, processing according to a program is realized on computer system.

[0046] The purpose, the description, and advantage of further others of this invention will become [rather than] clear by detailed explanation based on the example and the drawing to attach of this invention mentioned later. In addition, in this specification, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.

[0047]

[Embodiment of the Invention] Drawing which explains each entity in the contents use managerial system of this invention and the outline of processing of each entity to [system outline] drawing 1 is shown.

[0048] The user device 101 is the terminal of each user using contents, and, specifically, are regenerative apparatus, such as PC, a game terminal, and DVD, CD, a record regenerative apparatus, etc. These terminals are equipped with the security chip of the Tampa-proof configuration equipped with the control means which controls cipher processing explained in the latter part, and contents use processing. The service provider (SP-CD) 102 as a contents distribution entity (contents distributor), other entities, and many of processings that the user device 101 side in the data transfer performed between the user devices 101 is secure are controlled and performed within a security chip.

[0049] A service provider (contents distributor) (SP-CD) 102 is a service provider which offers contents to the user device 101 with a security chip. The contents creator 103 offers the contents for presenting service to a service provider (contents distributor) (SP-CD) 102. The user device manufacturer (Manufacturer) 104 is an entity which manufactures the user device 101.

[0050] A support center 105 is a center which performs the support to various processings with the user device with which the user device 101 was equipped, for example, performs various support processings to a user device, such as recovery processing of the password in the case of having forgotten the password which a user

uses as authentication information, or restoration (restoration) processing using the backup data of the contents which the user device generated. A certificate authority (CA:Certification Authority) 106 publishes a public key certificate (PKC:Public Key Certificate) to each entity.

[0051] In addition, the user device 101, a service provider (contents distributor) (SP-CD) 102, the contents creator 103, the user device manufacturer (Manufacturer) 104, a support center 105, a certificate authority (CA:Certification Authority) 106, and the number of each entities are arbitrary. Especially, although one certificate authority (CA:Certification Authority) 106 is shown in drawing 1 , two or more certificate authorities which publish the public key certificate for which a certificate authority is needed according to processing by each entity may exist.

[0052] In addition to this, the user device 101 receives satellite communication, the Internet communication link, or the contents enciphered from the service provider (contents distributor) 102 through the data communication network of a cable and wireless, and uses contents. key [for decoding encryption contents]: -- contents key: -- the contents use authority certificate as an authority information certificate in which Kc is enciphered and contents use authority is shown -- for example, in order to be stored in the attribute certificate (AC:Attribute Certificate) 110 and for a user terminal 101 to decode and use contents The attribute certificate (AC:Attribute Certificate) 110 is received from a service provider (contents distributor) 102, and it is necessary to take out and decode a key from an attribute certificate in a user device with a security chip.

[0053] the contents use authority certificate (AC:Attribute Certificate) 110, for example, the attribute certificate, as an authority information certificate in which contents use authority is shown The use limit information on contents, such as a count of a use limit, a use term, etc. of contents, other than Kc is recorded. The enciphered contents key : the user device 101 Use of the contents according to the contents use limit recorded on the attribute certificate (AC) 110 as a contents use authority certificate is attained.

[0054] In addition, hereafter, although explained as a configuration which stored the use information on contents, and an encryption contents key in the attribute certificate (AC:Attribute Certificate) 110, the certificate which stored the use information on contents and an encryption contents key can consist of explanation of an example as a certificate of the data format of not only an attribute certificate (AC) but the arbitration according to the so-called convention. That is, if it is the configuration that stored the data proving the use authority of contents and the

signature data of the issue entity for data alteration verification were added, the contents use authority certificate of the data format of arbitration is available.

[0055] In addition, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible.

[0056] Among each entity shown by drawing 1 , the entity of entities 101 other than certificate authority 106, i.e., a user device, a service provider (contents distributor) (SP-CD) 102, the contents creator 103 and the user device manufacturer (Manufacturer) 104, and a support center 105 performs processing by each entity according to the predetermined Ruhr in order to enable contents use and contents distribution according to the predetermined Ruhr. This Ruhr is set up and there is a system holder (SH:System Holder) which is not illustrated as an entity to manage. Each entity of 101-105 of drawing 1 performs processing by each entity under the contents use infrastructure which the system holder (SH) set up, and the Ruhr.

[0057] For example, the user device manufacturer (Manufacturer) 104 stores the device identifier (ID) applied in contents distribution in a security chip with the Tampa-proof configuration in the user device to manufacture, and various kinds of cipher-processing keys. In the contents transfer between the user device 101, a service provider (contents distributor) 102, the contents creator (CC) 103, and a support center 105, a transfer of an attribute certificate, and other data transfer processings, mutual recognition processing and data encryption processing are performed based on the Ruhr which the system holder (SH) set up.

[0058] Moreover, on the occasion of the contents use in the user device 101, contents use which observed the use limit recorded on the attribute certificate is performed. For example, processing which updates the counter which carries out the multiplier of the count of contents available to the bottom of control of the control section of the security chip in a device on the occasion of use of the contents to which the count limit was set is performed. The entity which builds and manages the platform which specified the Ruhr of processing by such each entity is a system holder (SH).

[0059] The outline is explained about the public key certificate and attribute certificate which are used in the configuration of [public key certificate and attribute

certificate] drawing 1 .

[0060] (Public key certificate (PKC)) A public key certificate is explained using drawing 2 , drawing 3 , and drawing 4 . A public key certificate is a certificate which a certificate authority (CA:Certification Authority) publishes, and when a user and each entity submit self ID, a public key, etc. to a certificate authority, it is a certificate with which a certificate authority side adds information, such as ID of a certificate authority, and an expiration date, adds the signature by the certificate authority further, and is created.

[0061] The example of a format of a public key certificate is shown in drawing 2 - drawing 4 . This is public key certificate format ITU-T. It is an example based on X.509.

[0062] A version (version) shows the version of a certificate format. A serial number (Serial Number) is a serial number of the public key certificate set up by the public key certificate issue station (CA). A signature (Signature) is the signature algorithm of a certificate. In addition, when there are an elliptic curve cryptosystem and RSA and the elliptic curve cryptosystem is applied as a signature algorithm, a parameter and key length are recorded, and key length is recorded when RSA is applied. A publisher (issuer) is the field where the publisher of a public key certificate, i.e., the name of a public key certificate issue office (IA), is recorded in an identifiable format (Distinguished Name). The initiation time and termination time whose expiration date (validity) is an expiration date of a certificate are recorded. As for subject public key information (subject Public Key Info), the algorithm of a key and a key are stored as a certificate owner's public key information.

[0063] A certification office key identifier (authority Key Identifier-key Identifier, authority Cert Issuer, authority Cert Serial Number) is information which identifies a certificate publisher's key used for signature verification, and stores the name of a key identifier and an engine certificate publisher, and an engine certificate serial number. A subject key identifier (subject key Identifier) stores the identifier for identifying each key, when proving two or more keys in a public key certificate. The key purpose of use (key usage) is the field which specifies the purpose of using a key, and each purpose of use for the signature check of the object for (0) digital signatures, the object for (1) denial prevention, the object for encryption of (2) keys, the object for encryption of (3) messages, the object for (4) common key delivery, the object for the signature check of (5) authentications, and (6) lapse list is set up. A private key expiration date (private Key Usage Period) records the expiration date of the private key corresponding to the public key stored in the certificate. A certificate authority policy (certificate Policies) records a public key certificate publisher's certificate

issue policy. For example, they are the policy ID based on ISO/IEC 9384-1, and authentication criteria. Policy mapping (policy Mapping) is the field which stores the information about limit of policy-related [under authentication pass], and is needed only for a certificate authority (CA) certificate. A subject alias name (subject Alt Name) is the field which records a certificate owner's alias name. A publisher alias name (issuer Alt Name) is the field which records a certificate publisher's alias name. A subject directory attribute (subject Directory Attribute) is the field which records the attribute of the directory needed for a certificate owner. Basic constraint (BASIC Constraint) is the field for the public key for certification to distinguish the object for the signature of a certificate authority (CA), and a certificate owner's thing. A permission subtree constraint name (name Constraints permitted Subtrees) is the field which stores the limit information on the identifier of the certificate which a publisher publishes. A constraint policy (policy Constraints) is the field which stores the limit information on the relation of the policy under authentication pass. The CRL reference point (Certificate Revocation List Distribution Points) is the field which describes the reference point of the lapse list of [for checking whether the certificate is invalidated and how it is], in case a certificate owner uses a certificate. A signature algorithm (Signature Algotithm) is the field which stores the algorithm used for signature attachment of a certificate. A signature is a public key certificate publisher's signature field. Electronic signature is data which generated the hash value with the application of the Hash Function to the whole certificate, and were generated using a publisher's private key to the hash value. Although the alteration is possible only by taking signature attachment and a hash, if detectable, there is effectiveness same with the ability not to alter substantially.

[0064] a certificate authority updates the public key certificate with which the expiration date went out, and performs creation of the lapse list (Revocation List) of [for excluding the user who performed injustice], management, and distribution (this -- RIBOKESHON: -- referred to as Revocation) while it publishes the public key certificate shown in drawing 2 - drawing 4 . Moreover, generation of a public key and a private key is also performed if needed.

[0065] On the other hand, in case this public key certificate is used, using the public key of the certificate authority which self holds, a user verifies the electronic signature of the public key certificate concerned, after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate, and uses the public key concerned. Therefore, all the users using a public key certificate need to hold the public key of a common certificate authority.

[0066] (Attribute certificate (AC)) An attribute certificate is explained using drawing 5 . It roughly divides into an attribute certificate, there are two classes, and one is a certificate including the attribute information of the owner about the right and authority of the right of use of contents. Another is an attribute certificate for partitioning for (service providers SP), or deletion (AC), and is an attribute certificate (AC) including partitioning in the case of securing or deleting the information storing field for (service providers SP) in the memory in a user device, or the consent information on deletion.

[0067] The attribute certificate format is prescribed by ITU-T X.509, and has decided upon Profile by IETF PKIX WG. Unlike a public key certificate, an owner's public key is not included. However, since the signature of an attribute certificate certificate authority (Attribute Certificate Authority) sticks, the point that the judgment of whether to be altered can be performed by verifying this signature is the same as that of a public key certificate.

[0068] As for the attribute certificate certificate authority (Attribute Certificate Authority) which performs issue management of an attribute certificate (AC), in the configuration of this invention, it is possible for a service provider (contents distributor) (SP-CD) 102 to hold an additional post. It is good also as another configuration. An attribute certificate is always related with a public key certificate, and is used. That is, it is the attribute certificate which this human nature of an owner itself is checked with a public key certificate, and what kind of authority is granted to the owner on it, or shows a chisel. After performing signature verification of the certificate concerned in verification of an attribute certificate, verification of the public key certificate related with it is also performed.

[0069] In addition, it is desirable in that case that follow a certificate chain in principle and even the top public key certificate verifies in order. Two or more certificate authorities (CA) exist, and the public key certificate of a certificate authority own [low-ranking] is signed with the certificate authority configuration which makes hierarchy organization by the high order certificate authority which publishes the public key certificate. That is, a chain of public key certificate issue configuration that the public key certificate issue station (CA-High) of a high order publishes a public key certificate to a lower layer public key certificate issue station (CA-Low) is taken. Chain verification of a public key certificate means following a certificate chain from low order to a high order, acquiring the chain information to the top public key certificate, and performing signature verification of the public key certificate to the most significant (root CA).

[0070] By the shelf-life of an attribute certificate being a short period of time, it is also possible not to perform lapse processing. In this case, the lapse procedure of a certificate, the reference procedure of lapse information, etc. can be skipped, and there is the advantage from which a system becomes simple. However, since a certain cures other than a lapse are needed to unjust use of a certificate, it must fully be careful. In this authentication system, since it is the configuration which embeds the contents key for decoding the contents other than use authority to contents in the attribute certificate, the user device with just contents use authority is available in contents by receiving a just attribute certificate.

[0071] The configuration of the attribute certificate shown in drawing 5 is explained. The version number of a certificate shows the version of a certificate format. AC holder's public key certificate information and this are the information about the public key certificate (PKC) corresponding to the publisher of an attribute certificate (AC), and are information, such as a PKC publisher name, a PKC serial number, and a PKC publisher proper identifier, and it has a function as link data which associate a correspondence public key certificate. The identifier of the publisher of an attribute certificate is the field where the publisher of an attribute certificate, i.e., the name of an attribute certificate certificate authority (AA), is recorded in an identifiable format (Distinguished Name). A signature algorithm identifier is the field which records the signature algorithm identifier of an attribute certificate. The initiation time and termination time whose expiration date of a certificate is an expiration date of a certificate are recorded. According to the use gestalt of an attribute certificate, as for attribute information field, either (1) memory area reservation, deletion information or (2) contents use condition related information is stored. The enciphered contents key is included in contents use condition related information.

[0072] (1) Memory area reservation and deletion information are recorded on the attribute certificate with which a service provider is published for the purpose of a registration setup or deletion in the management domain for every service provider by the memory in the security chip of a user device. Recording information is the following information.

Service provider identifier (ID)

Service-provider name processing: Memory area reservation and memory area deletion are the size [0073] of an area-size:memory area either. A service provider sends the attribute certificate which stored each above-mentioned item in attribute information field to a user device, and a user device performs secured processing of a memory area in which record of the attribute information field of the attribute

certificate received in the memory after verification of an attribute certificate and in the security chip of self was followed, or deletion of a memory area [finishing / reservation].

[0074] (2) Contents use condition related information is information stored in the attribute information field of the attribute certificate published corresponding to the contents which a service provider offers, and contains the encryption data of the contents key which enciphered contents further including various use conditions, such as a count of a use limit of contents, and a use term. Recording information is the following information.

Service provider identifier (ID)

Service-provider name application identifier (ID): It is the identification information of contents.

Conditions: It is the information which shows [online use contents, off-line use contents, and] any of buying-up contents, time limitation contents, the count limit contents of online, and the count limit contents of off-line they are further.

expiration date: -- count [in the case of time limitation] of expiration date information use limit: -- count payment condition [in a count limit / of available]: -- the payment condition of the countervalue of contents -- record contents key: -- the enciphered contents key -- encryption algorithm information -- storing [0075] There is each mode of the mode which buys up and carries out (a) contents like a publication in the above-mentioned condition field at the use mode of contents with distinction of (1) online use and (2) off-line use, and makes contents use after buying up free, the mode which prepared (b) time limitation and set up the use period of contents, and the mode which prepared the count limit of (c), and restricted the count of use of contents. Moreover, there is also a combination limit mode accompanied by both limits of time limitation and a count limit. In a user device, use of contents is performed according to these modes recorded on the attribute certificate. The latter part explains these concrete processing modes.

[0076] Moreover, the contents key applied as a decode key of encryption contents: The encryption contents key which enciphered Kc is stored. Contents key: The main classes of key applied to encryption processing of Kc directly or indirectly are as being shown below.

(a) Storage public key:SC.Stopub.SP.K corresponding to the (service provider SP) corresponding to the storage private key corresponding to SP stored in each service provider management domain of the security chip of a user device (public key system),

(b) The storage key corresponding to SP stored in each service provider management

domain of the security chip of a user device (common key system)
(c) private key: which a service provider holds -- global common key:kg generated as a key shared between an SP.Sto.K(d) system holder (SH) and a user device -- the latter part explains the processing which applied these keys to a detail.
[0077] Further, a signature algorithm is recorded on an attribute certificate and a signature is performed to it by the attribute certificate certificate authority (AA) which is an attribute certificate publisher. Electronic signature is data which generated the hash value with the application of the Hash Function to the whole attribute certificate, and were generated using an attribute certificate publisher's (AA)'s private key to the hash value.
[0078] [Security chip configuration] The configuration of the security chip constituted in the user device as an information processor which uses contents next is explained referring to drawing 6 . In addition, a user device will be constituted by regenerative apparatus, such as CPU as a data-processing means, PC equipped with communication facility, a game terminal, and DVD, CD, the record regenerative apparatus, etc., and the security chip which has the Tampa-proof structure in these user devices will be mounted. The example of a configuration of the user device itself is explained in the tail of this specification. The user device with a security chip is manufactured in the user device manufacturer 104 in drawing 1 .
[0079] As shown in drawing 6 , the security chip 210 is mutually built in the user device 200 to the user device side control section 221 as a configuration in which data transfer is possible. The security chip 210 has CPU (Central Processing Unit)201 with a program execution function and a data-processing function. The communication interface 202 with the interface function for data communication, the various programs performed by CPU201, For example, ROM (Read Only Memory)203, the load field of an executive program which memorize master key:km stored at the time of manufacture of a code processing program and a device, Moreover, authentication processing with RAM (Random Access Memory)204 and the external instrument which function as a work-piece field in each program manipulation, The cipher-processing section 205 which performs cipher processing, such as generation of electronic signature, verification processing, a storing data encryption, and decryption processing, the information for every service provider mentioned above, It has the memory section 206 which stored the proper information on the device containing various key data and which is constituted by EEPROM (Electrically Erasable Programmable ROM), for example. About the detail of these storing information, it mentions later.

[0080] The user device 200 has the external memory section 222 constituted with EEPROM as a field which stores encryption contents etc., a hard disk, etc. The external memory section 222 is available also as a storing field of a public key certificate and an attribute certificate, and is used also as a storing field of the count management file of use of the contents explained in the latter part.
[0081] When the user device carrying a security chip connects with an external entity, for example, a service provider, and it performs data transfer processing, if needed, the security chip 210 and mutual recognition between external entities are performed, and a transfer data encryption is performed. The detail of these processings is explained in full detail in the latter part.
[0082] The example of data used as the processing object in the security chip of a user device is shown in drawing 7 . Although these many are stored in the memory section 206 constituted by EEPROMs (Electrically Erasable Programmable ROM), such as a flash memory which is one gestalt of nonvolatile memory, it stores at the time of manufacture, and it is stored in ROM (Read Only Memory)203 data [of which rewriting is made impossible], for example, master key:, km. A public key certificate and an attribute certificate may be stored in the memory in a security chip, or may be stored in external memory.
[0083] Each data is explained.
Public-key certificate (PKC): A public key certificate is a certificate in which it is shown to a third person that it is a just public key, and the digital signature is carried out to the certificate by the certificate authority which can set reliance including the public key to distribute. The public key certificate of the service provider registered into the public key certificate of the top certificate authority (root CA) of the hierarchy organization mentioned above and the user device, i.e., the service provider from which the memory area is secured in the user device, and the public key certificate of the support center which performs the support of password return processing etc. further are stored in a user device.
[0084] Attribute certificate (AC): An attribute certificate shows a certificate user's use authority to a public key certificate showing the certificate user's (owner) "this human nature." By showing an attribute certificate, a user can perform use of application, reservation of a field, etc. now based on the right and authority indicated by the attribute certificate. Below, below the class of attribute certificate is shown and each role to play is shown.
[0085] (a) Application use administrative attribute certificate (AC) : it is the expression which used the contents generally called application in large semantics,

and there are various applications, such as a game, music, a movie, and financial information, as a class of application. With an application use administrative attribute certificate (AC), there is description about the use authority of application, an attribute certificate (AC) is shown to a service provider (SP), it is local and use consent of the application in use authority within the limits described by the attribute certificate (AC) verification or by verifying is obtained. or online use of application is possible or off-line use is possible as description about the use authority of application -- further -- online -- the case of available contents -- use time limitation and the count limit information of use -- it is -- off-line -- in being available contents, there are a count limit of use and description which shows buying up.

[0086] (b) The attribute certificate for memory area management (reservation) for (service providers SP) (AC) : when registering a service provider (SP) into a user device, it is necessary to secure the information storing field about SP in a user device. The consent information on partitioning at this time is stored in an attribute certificate (AC), and the field for SP is secured in a user device in a user device according to the information stored in the attribute certificate (AC).

[0087] (c) The attribute certificate for memory area management (deletion) for (service providers SP) (AC) : it is the attribute certificate (AC) which stored the consent information on deletion of the field for SP secured in the user device. In a user device, deletion of the field for SP in a user device is performed according to the information stored in the attribute certificate (AC).

[0088] Key data: The key for random-number generation, the key for mutual recognition, etc. are stored in the storage key and pan which are used as a key for cipher processing in the case of data storage, such as a pair of the public key set up to a device as key data, and a private key, and contents.

[0089] A storage key is a key of encryption of the contents key saved at a device, or decryption processing applied to either at least. There are a storage key corresponding to a device and a storage key corresponding to a service provider, and the storage key corresponding to a service provider is a key stored in each service provider management domain for every service provider of each which was registered into the device, and is applied to a storage key corresponding to the contents key which a corresponding service provider offers. The global common key constituted as a key which only a device shares with a system holder is contained, and a global common key is used for the storage key corresponding to a device in case message distribution processing of the encryption contents key which prevented the decryption processing in a service provider is performed. The latter part explains the

detail of the processing which applied these keys.

[0090] Identification information: In addition, user ID can give the user ID given to the user who uses the service provider ID and user device as the device ID as an own identifier of a user device, and an identifier of the service provider (SP) registered into the user device as identification information, and different user ID for every external entities, such as a service provider. Application ID is ID as identification information corresponding to the service and contents which are offered by the service provider (SP).

[0091] Others: The authentication information (for example, password) for obtaining further use consent of the service provider (SP) information registered into the user device as authentication information is stored in a user device. By entering a password, it becomes acquirable [the service provider (SP) information registered into the user device], and use of the application which a service provider offers, and contents is permitted after information acquisition. When authentication information (password) has been forgotten, initialization (reset) processing of authentication information (password) is possible using a master password.

[0092] The seed information further for random-number generation is stored. A random number is ANSI in the cases, such as authentication processing and cipher processing. It generates according to X9.17.

[0093] Furthermore, the hash value computed based on the count information of contents use or the count information of contents use is stored. This is information which is needed in order to perform strictly contents use within the count limit of use stored in the attribute certificate corresponding to application and contents, and saves the application ID as identification information of the attribute certificate corresponding to contents, the serial number of an attribute certificate, and the count of a use limit of contents. Although the alteration is possible only by taking signature attachment and a hash, if detectable, there is effectiveness same with the ability not to alter substantially.

[0094] Although some various data [at least] mentioned above are stored in the memory section 206 constituted by EEPROMs (Electrically Erasable Programmable ROM), such as a flash memory which is one gestalt of [memory configuration in user device] nonvolatile memory, these are classified into three fields by which division management was carried out, i.e., (1) device management domain, (2) system-management field, and (3) service provider management domain, and are stored in memory section 206 field. Hereafter, the storing data for every fields of these are explained.

[0095] (1) The information which does not depend for a device management domain device management domain on the system of a device proper is held. This field is a field which a field is first secured at the time of device manufacture, and occupies two or more blocks of the head of nonvolatile memory. In a device management domain, the following data are held and managed at least.
device ID random-number generation -- the ** storage key for seed random-number generation corresponding to a cryptographic key mutual recognition key device [0096] A mutual recognition key is a key for authentication with the entity used as an output destination change, when outputting the data in a security chip to the security chip exterior. In addition, an entity also contains the user device equipped with a security chip which are regenerative apparatus, such as a game terminal, and DVD, CD, and a record regenerative apparatus, for example. Mutual recognition processing which applied the mutual recognition key at the time of the data transfer between user devices with a security chip and a security chip and data communication with the service provider of the exterior which minded the user device further etc. is performed. It enciphers with the session key generated the condition [formation of mutual recognition] at the time of mutual recognition, and data transfer between the interior of a security chip and the exterior is performed.
[0097] The storage key corresponding to a device is a key for enciphering data and preventing perusal and an alteration, when holding the data inside a security chip outside. A public key system, a common key system, or whichever is sufficient as a device storage key. In case the seed for random-number generation asks for the pseudo-random number by arithmetic operation, he is data used as initial seed. Arithmetic operation of the pseudo-random number is carried out using the cryptographic key for random-number generation, and a random number is generated.
[0098] The global common key constituted as a key which only a device shares with a system holder is contained, and a global common key is used for the storage key corresponding to a common key system device in case message distribution processing of the encryption contents key which prevented the decryption processing in a service provider is performed. The latter part explains a global common key to a detail.
[0099] (2) A system management field system management field is secured in a memory area as well as a device management domain. The following data are held and managed in a system management field.
Root (certificate authority CA) public key certificate device public key certificate device private key [0100] When the root (certificate authority CA) public key

certificate is a certificate used as the origin of all the authentication systems in a security chip, follows signature verification of other certificates and performs the above-mentioned chain verification, finally it will arrive at the public key certificate of a root certificate authority (CA).

[0101] A device public key certificate is a public key certificate used at the time of mutual recognition with a service provider. When generating and importing a device private key externally, a device public key certificate is also generated by coincidence. When generating a device private key and a public key by the device side, after a device private key and a public key are generated within a device, a device public key is read from a device, issue processing of a device public key certificate is performed, and import of the published device public key certificate is performed.

[0102] A device private key is a key for and attesting to data. [signature] Although a private key is generated in a public key and a pair, it is generated externally beforehand, is generated inside whether it considers as the configuration imported to a device secure one, and a device, and is considered as one configuration of whether it considers as the configuration never taken out outside.

[0103] (3) A service provider management domain service provider (SP) management domain consists of a (service provider SP) managed table and service provider (SP) management information. A (service provider SP) managed table is a table to show the whereabouts of each service provider (SP) information in a (service provider SP) management domain, is made to correspond to the identifier of a service provider, and has the storing positional information of each service provider (SP) information on memory.

[0104] in addition -- a service provider (SP) management domain -- a user device -- a service provider -- (-- performing member registration to every SP) -- a service provider -- (-- the field of every SP) is secured in the memory area in a device. In addition, partitioning or deletion is performed based on description of an attribute certificate. The following information is held in a service provider (SP) management domain.

[0105] The storage private key corresponding to the private key (service provider SP) corresponding to (a service provider SP) (public key system)
The storage key corresponding to (a service provider SP) (common key system)
Count management data authentication information User Information of hash value contents use of external management information [0106] The private key corresponding to (a service provider SP) is a private key of the pair of a public key and a private key applied to mutual recognition processing with a registration service

provider (registration service provider (SP who generated corresponding to every SP)), or encryption data transfer processing. It is the key needed when a registration service provider (SP) and a security chip carry out mutual recognition.

[0107] Whenever the storage private key (public key system) corresponding to (a service provider SP) uses the contents which acquired off-line the contents use which a service provider offers when available, when it is the contents which do not need connection with a service provider, it is a key for decode of the encryption contents key corresponding to contents. In a service provider, it is enciphered with the storage public key corresponding to the (service provider SP) corresponding to the storage private key corresponding to (a service provider SP), is stored in an attribute certificate (AC), and is transmitted to a user device, and within the security chip of a user device, an encryption contents key is decoded with the storage private key corresponding to (a service provider SP), and becomes acquirable [a contents key].

[0108] Whenever the storage key (common key system) corresponding to (a service provider SP) uses the contents which acquired off-line the contents use which a service provider offers when available, when it is the contents which do not need connection with a service provider, it is a key for decode of the encryption contents key corresponding to contents, and is a key applicable to encryption and decryption processing in common. In addition, the storage private key (public key system) corresponding to (a service provider SP) and the storage key (common key system) corresponding to (a service provider SP) are good also as a configuration which stores and applies only either. .

[0109] It is made to be not possible [the alteration of the hash (Hash) value of external management information] by taking out the data which are too large for managing inside a security chip to the specific region of external memory, and managing the hash value of the field within a security chip. For example, when applying a count use limit of contents, the number of ** times etc. serves as an administration object by the hash value. In the case of count management contents, the perusal of count information itself is satisfactory, but an alteration must be prevented. Although the alteration is possible only by taking signature attachment and a hash, if detectable, there is effectiveness same with the ability not to alter substantially.

[0110] A security chip is local and the count of available of the count management data application of contents use (contents) may be managed. At this time, the serial of Application ID and an attribute certificate (AC) and the count of available are held and managed inside a security chip. The latter part explains management processing of the

count management data of contents use to a detail.

[0111] Authentication information authentication information is information to protect the management information managed in a service provider (SP) management domain. Although, as for a user, mutual recognition with a service provider (SP) is needed at the time of (service provider SP) connection, information required for mutual recognition is stored in a service provider (SP) management domain. It is the authentication information which is used in order to acquire required information from this management domain. Specifically, authentication information is a password. When the user has forgotten authentication information (password), use consent of the management information of a service provider (SP) management domain is no longer obtained. In this case, by inputting a master password, reset of the authentication information itself is performed and a change can be made. The latter part explains these processing configurations to a detail.

[0112] User Information User Information is user proper information, such as user ID assigned by the service provider (SP).

[0113] Below [password management], the user device 101 shown in drawing 1 receives the contents which a service provider (contents distributor) 102 offers, and the detail of various processings which is needed on the occasion of the processing using contents and contents use under the use limit according to an attribute certificate is explained. First, the authentication information for the access controls to the service provider management domain of the memory area in the user device who stored the information about the service provider which offers contents (password) is explained.

[0114] (1) In order for the user who purchased the authentication information (password) registration processing user device to perform processing using the contents which purchase contents from various service providers under management of a system holder and which were processed or purchased, set a service provider management domain as the memory area in a user device, and the processing which stores the management information for every service provider in this service provider management domain is needed. The service provider by which the service provider management domain was set as the memory area in a user device is called a registration service provider below. The above-mentioned attribute certificate is applied to a setup of a service provider management domain, and setting processing of a service provider management domain in which record of an attribute certificate was followed in the memory area in a user device is performed to it based on the attribute certificate which the user device received from the service provider.

[0115] In order for a user device to access and to perform the purchase of contents, or use to a registration service provider with a service provider management domain, it is necessary first to acquire the information in the service provider management domain in a user device. It is because it is necessary to store information required for the mutual recognition processing between a user device and a service provider in the service provider management domain, to acquire such information, and to perform mutual recognition with a service provider.

[0116] In order to access this service provider management domain, it is necessary for a user to input the authentication information (password) set up for every registration service provider through the input means of a user device. In addition, in the following explanation, the description with "every service provider" is synonymous with "every registration service and every user." It restricts, when coincidence verification of an input password and a registration password is performed and it is in agreement by the security tip side, and the information acquisition in the service provider management domain formed in the memory in a security chip is attained, and access with a subsequent service provider through which mutual-recognition-processes and it passes is attained.

[0117] Authentication information (password) is set up for every service provider registered into the user device. The user itself performs initial registration of these passwords. Initial registration processing of a password is explained with reference to drawing 8 . In the sequence diagram of drawing 8 , it is user interface side processing in the user device in which left-hand side has a security chip, and right-hand side has a security chip.

[0118] First, the corresponding service provider used as the candidate for (1) password registration is specified, and a user inputs the initial registration processing initiation demand of authentication information (password). (2) In the security tip side, when the service provider which the user specified performs whether it is a registration service provider [finishing / a setup of a management domain / already], and is in the condition by which a password setup is not carried out, and status check processing in the memory in a security chip and these are checked, permit initial registration processing of (3) authentication information (password).

[0119] Next, a user minds input means, such as a keyboard, from a user interface side. (4) Enter a password and the control section of (5) security chip holds the inputted authentication information (password) in memory temporary. (6) If the reinput demand of the same password is performed and reinput of authentication information (password) is made by (7) users (8) when the control section of a security chip

performs collating of reinput authentication information (password) and the authentication information (password) currently held in memory temporary and collating is materialized (9) Write-in processing of authentication information (password) is performed, and a user is notified of a (10) write-in result, and if it is O.K., it ends. (11) In the case of NG, return to processing of (1).

[0120] (2) The sequence diagram of modification processing of a password is shown in authentication information (password) modification processing drawing 9 and drawing 10 . A password change has two processing modes, the modification processing (at the time [Usually]) which used the registered password, and the modification processing (emergency) using a master password.

[0121] First, based on the sequence diagram of drawing 9 , the password change processing at the time, i.e., the modification processing using a registered password, is usually explained. It is user interface side processing of the user device in which left-hand side has a security chip, and right-hand side has a security chip.

[0122] First, the corresponding service provider used as (1) password-change processing object is specified, and a user inputs an authentication information (password) modification processing initiation demand. (2) a condition [checked / processed the status check and / whether you are SP who is a registered service provider (SP) and by whom the service provider which the user specified had the management domain set as memory, and the password was set up in the security tip side, and / these] -- carrying out -- (3) -- perform a registered authentication information (password) input request. A user enters (4) registered password through input means, such as a keyboard, from a user interface side, and the control section of (5) security chip will perform collating processing with the registration authentication information (password) currently written in the service provider management domain, if an input is checked.

[0123] Formation of collating notifies (6) modification processing authorization. A user minds input means, such as a keyboard, from a user interface side. (7) Input new authentication information (password) and the control section of (8) security chip holds the inputted authentication information (password) in memory temporary. (9) If the reinput demand of the same password is performed and reinput of authentication information (password) is made by (10) users (11) when the control section of a security chip performs collating of reinput authentication information (password) and the authentication information (password) currently held in memory temporary and collating is materialized (12) Write-in processing of authentication information (password) is performed, and a user is notified of a (13) write-in result, and if it is O.K.,

it ends. (14) In the case of NG, return to processing of (1).

[0124] (3) Explain the authentication information (password) reset processing using the master password performed in the password change processing in emergency etc. based on the authentication information (password) reset processing using a master password, next the sequence diagram of drawing 10 . It is user interface side processing in the terminal equipped with the user device in which left-hand side has a security chip, and right-hand side has a security chip.

[0125] First, the corresponding service provider used as (1) password-change processing object is specified, and a user inputs an authentication information (password) reset processing initiation demand. (2) When the service provider which the user specified processes whether you are SP who is a registered service provider (SP) and by whom the management domain was set as memory, and the password was set up, and a status check and is satisfied with the security tip side of these conditions, perform (3) master-password input request. A user inputs (4) master passwords through input means, such as a keyboard, from a user interface side, the control section of (5) security chip performs collating processing of the inputted master password, and it judges whether it is the input of a right master password, and if it judges with it being a right master password input as a result of verification, it will perform in initialization of the registration authentication information (password) currently written in (6) service-provider management domain, i.e., the reset processing of registered authentication information (password).

[0126] The control section of a security chip notifies a user of the notice of (7) processing result after reset processing, and if it is O.K., a user will perform the above-mentioned authentication information (password) registration processing, for example. Since these processings are the same as the processing previously explained with reference to drawing 8 , explanation is omitted. (8) When a reset processing result is NG, return to processing of (1).

[0127] As explained using the processing sequence of drawing 10 , a master password is applied, in case it initialization-processes, namely, authentication information (password) registered about each registration service provider resets. The authentication information initialization (reset) processing using a master password is effective to the authentication information on all the service providers registered into the security chip.

[0128] The related Fig. of a master password and the authentication information on each registration service provider (password) is shown in drawing 11 . As shown in drawing 11 , it exists as a high order password to each authentication information

corresponding to a service provider, initialization (reset) of the authentication information on a registration service provider (password) is respectively performed by the input of a master password, and a master password becomes possible [re-registering new authentication information as authentication information on each registration service provider (password)].

[0129] The form printed, for example at the time of the purchase of a user device is attached to a device, and a master password is distributed, as shown in drawing 12 . Although a master password is written in at works at the time of manufacture of a device, read-out from the device of the master password by the user has impossible composition. A master password is generated by the device based on the device ID which is the identifier of a proper, and a master key. a master key -- information-processor each or a group -- it is the key set up corresponding to an information processor.

[0130] When the user has forgotten the master password, recurrence line processing of a master password is attained a condition [the registration to a support center]. The recurrence line processing sequence diagram of the user registration processing and the master password to a support center is shown in drawing 13 .

[0131] The upper case of drawing 13 shows the user registration processing sequence diagram to a support center. A user can connect with a support center through the terminal which set up mailing of the registration form attached to the purchase device, or a device, and can perform user registration. If user registration is performed as processing which registers data, such as ID of the user address, the telephone number, and a device, into a support center and user registration is completed in a support center, the notice of user registration completion will be sent or transmitted to a user from a support center.

[0132] The lower berth of drawing 13 is the sequence of the master password recurrence line processing performed between support centers with a user, when the user has forgotten the master password. If a user transmits the recurrence line demand of a master password to a support center with the User Information data accompanied by a device ID and a support center receives a demand, it judges whether User Information and user ID of a support center correspond with registered data, and when in agreement, retrieval of the master password based on a user device ID or generation processing of the master password using a master key will be performed. A support center has the master password storing database to which the device ID as a device identifier set up corresponding to the user device as an information processor and the master password were made to correspond. or a device

ID and device each -- the key of a proper, or a group -- in having either of the master key storing databases to which the master key set up as a key common to a device was made to correspond and having a master password storing database, a database search is performed based on a device ID, and it acquires a master password. In having a master key storing database, master password generation processing by cipher processing which applied the master key to a device ID is performed, and it performs processing which sends the generated master password to a user device.

[0133] The generation processing flow of a master password with the master key based on a user device ID is shown in drawing 14 . The flow of drawing 14 is explained. First, in step S101, encryption processing of a device ID is performed using a master key Km1. The result is set to MPa in step S102. furthermore, a result -- MPa -- receiving -- the master key Km2 -- having applied -- encryption -- processing -- performing -- Password MP -- obtaining -- step S -- it changes into an ASCII code in 103. Encryption algorithms, such as DES and Triple DES, can apply encryption processing. Master keys Km1 and Km2 are keys set up in common to two or more devices, and a support center chooses and uses the master key which should be applied from two or more keys held in a support center based on a user device ID.

[0134] It returns to the sequence diagram of drawing 13 , and explanation is continued. If generation of a master password is performed in a support center, a support center will transmit or send a master password to a user or a user device online or off-line.

[0135] According to the above sequence, a user can perform recurrence line processing of a master password using a support center. In addition, as for a user device and restricted data which perform, transmit and receive mutual recognition processing as pretreatment of data transmission and reception between support centers, for example, user ID, a master password, etc., it is desirable to encipher by the session key generated at the time of mutual recognition, and to perform generation of a signature and verification for alteration prevention of data. In addition, the item of the message distribution processing of contents explains details, such as these mutual recognition processing, signature generation, and verification processing, in detail.

[0136] Moreover, a user can also perform recurrence line processing of the master password using a support center off-line. in this case, a postcard etc. -- him -- processing of filling in and sending the information for a check will be performed.

[0137] If the management domain of a service provider is registered into the memory area in the security chip in a [contents message distribution processing] user device and information required for authentication with a service provider, the

above-mentioned password, etc. are registered, the contents purchase by the communication link with a service provider will be attained using such information. Hereafter, the detail of contents purchase processing is explained.

[0138] The sequence diagram explaining the outline in contents purchase processing is shown in drawing 15 . It is the user device side processing in which left-hand side has a security chip, and right-hand side is service provider side processing.

[0139] A user device outputs the purchase demand of contents to a service provider first. A service provider's reception of a contents purchase demand performs mutual recognition between a user device and a service provider. If mutual recognition is materialized and both justification is checked, a service provider will generate the attribute certificate (AC:Attribute Certificate) corresponding to purchase demand contents, and will transmit to a user device. The contents key for decoding contents in an attribute certificate: Kc is enciphered, and it is stored and contents use conditions, such as a count of use and a use term, are recorded. Moreover, the signature of the attribute certificate certificate authority (AA:Attribute Certificate Authority) which is an attribute certificate publisher is made to storing data, and it has become a thing in consideration of alteration prevention.

[0140] The user device which received the attribute certificate performs signature verification processing of an attribute certificate, and saves an attribute certificate in memory based on the judgment without an alteration. Furthermore, the contents key stored in the attribute certificate which the user device gave the demand of contents to the service provider, and sent the service provider to the user device previously: Send the contents enciphered by Kc to a user device. In a user device side, decryption processing of the enciphered contents key which was picked out from the attribute certificate is performed, contents are acquired by decryption processing of the encryption contents which applied the contents key which took out and took out the contents key, and it uses. In addition, there is also a mode (online decode) which performs decryption processing of the contents key stored in the attribute certificate by the service provider side. The latter part explains these examples of concrete processing.

[0141] The rough flow accompanying contents distribution is as having explained using drawing 15 above. Hereafter, the detail of each processing is explained. In addition, although the attribute certificate corresponding to contents is performed at the point of encryption contents sending in the processing sequence shown in drawing 15 , distribution of encryption contents and distribution of an attribute certificate are good also as processing which the point is sufficient as any and they distribute to

coincidence. Moreover, it is also possible to consider as the configuration which performs off-line distribution which stores each in record media, such as a disk, and distributes it.

[0142] Moreover, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand.

[0143] (1) Between mutual recognition processing, the user device which is the purchase demand entity of contents, and the service provider which is the offer origin of contents, mutual recognition processing is performed first. Between two means to perform data transmission and reception, it is performed that a partner checks mutually whether you are a right data communication person, and performs required data transfer mutually after that. Check processing of whether a partner is a right data communication person is mutual recognition processing. The configuration which performs encryption processing by using as a share key the session key which performed generation of a session key and was generated at the time of mutual recognition processing, and performs data transmission is one desirable data transfer method. As a mutual recognition method, application of all directions types, such as a public key cryptosystem and a common key encryption system, is possible.

[0144] Here, the handshake protocol (TLS1.0) which is one authentication mode of processing of a public key cryptosystem is explained with reference to the sequence diagram of drawing 16 .

[0145] In drawing 16 , left-hand side shows processing of a user device (client), and right-hand side shows the processing by the side of a service provider (server). First, it transmits to a user device (client) by giving a negotiation initiation demand for (1) service provider (server) determining an encryption specification to a halo request. (2) A user device (client) will be transmitted to a service provider (server) side by making the candidate of encryption algorithm, Session ID, and a protocol version who uses into a client halo, if a halo request is received.

[0146] (3) A service provider (server) side transmits to a user device (client) by making into a server halo the encryption algorithm, Session ID, and the protocol version which opted for use. (4) A service provider (server) transmits a package of a

public key certificate (X. 509v3) to Root CA which self owns to a user device (client) (server certificate). In addition, when a certificate chain is followed and even the top public key certificate does not verify in order, it is not necessary to necessarily send a package of a public key certificate (X. 509v3) to Root CA. (5) A service provider (server) transmits a RSA public key or Diffie&Hellman public key information to a user device (client) (server key exchange). This is public key information applied temporarily, when a certificate cannot be used.

[0147] (6) Next, to a user device (client), as a certificate request, a service provider (server) side requires the certificate which a user device (client) has, and tells termination of the negotiation processing by (7) service providers (server) (server halo termination).

[0148] (8) The user device (client) which received server halo termination transmits a package of a public key certificate (X. 509v3) to Root CA which self owns to a service provider (server) (client certificate). In addition, when not performing chain verification of a public key certificate, package sending of a public key certificate is not indispensable. (9) A user device (client) enciphers a 48-byte random number with the public key of a service provider (server), and transmits it to a service provider (server). A service provider (server) and a user device (client) generate the master secret which contains the data for the message authorization code:MAC (Message Authentication Code) generation for transmitted-and-received-data verification processing etc. based on this value.

[0149] (10) in order that a user device (client) may check the rightness of a client certificate -- the digest of the message so far -- the private key of a client -- enciphering -- a service provider (server) -- transmission (client certificate check) -- carrying out -- (11) -- notify initiation of the encryption algorithm determined previously and key use (change cipher spec.), and notify termination of (12) authentications. On the other hand, initiation of the encryption algorithm previously determined from (13) service-provider (server) side also to the user device (client) and key use is notified (change cipher spec.), and termination of (14) authentications is notified.

[0150] According to the encryption algorithm determined in the above-mentioned processing, data transfer between a user device (client) and a service provider (server) will be performed.

[0151] Verification of a data alteration performs alteration verification of a message by adding message authorization code:MAC (Message Authentication Code) computed from the master secret generated by the basis of agreement between a user device

(client) and a service provider (server) by above-mentioned authentication processing to the transmit data of each entity.

[0152] drawing 17 -- message authorization code: -- the generation configuration of MAC (Message Authentication Code) is shown. A data source adds the MAC secret generated based on the master secret generated in authentication processing to transmit data, calculates a hash value from these whole data, performs hash calculation based on a MAC secret, padding, and a hash value further, and generates a message authorization code (MAC). When this generated MAC is added to transmit data, it will judge with having no data alteration if coincidence with MAC and Reception MAC which were generated based on received data by the receiving side is accepted, and coincidence is not accepted, it judges with a thing with the alteration of data.

[0153] (2) The contents key which can apply the service provider by which the demand of contents was made to decryption processing of demand contents from generation of a contents use authority information certificate (attribute certificate), and a sending-user device : generate the contents use authority information certificate which enciphered and stored Kc and stored the use limit information on contents, for example, an attribute certificate, (AC), and transmit to a user.

[0154] Even if the subject who generates a contents use authority information certificate (AC), for example, an attribute certificate, is the service provider itself, he may be an external entity which performs contents management. When an external entity generates an attribute certificate (AC), according to the demand of a service provider, the external entity generates an attribute certificate (AC).

[0155] A contents key applicable to an attribute certificate at decode of correspondence encryption contents: Kc is enciphered and stored. In the lock applied to encryption of the contents key Kc For example (a) The private key which the storage public key:SC.Stopub.SP.K (b) service provider corresponding to the (service provider SP) corresponding to the storage private key corresponding to SP stored in each service provider management domain of the security chip of a user device holds : (Common key system) There is each global common key:kg mode generated as a key shared between an SP.Sto.K(c) system holder (SH) and a user device. In addition, some modes in addition to this are possible. For example, it is also possible to encipher with the public key which a service provider holds. In this case, it will decrypt with the private key which receives an attribute certificate (AC) from a user device, and a service provider holds.

[0156] In addition, even when which encryption mode is applied, as a distribution

gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand. Hereafter, the detail of the processing in the mode of above-mentioned (a) - (c) is explained.

[0157] (a) The storage public key corresponding to the (service provider SP) corresponding to the storage private key corresponding to SP : as it is under explanation about the memory area of the security chip of the user device mentioned above when SC.Stopub.SP.K was applied and was shown, storage private key:SC.Stopri.SP.K corresponding to SP is stored in each service provider management domain formed in memory about each registration service provider registered into the user device. With the security chip of a user device the service provider corresponding to the storage private key corresponding to SP out of the attribute certificate corresponding to the contents offered from a service provider -- contents key:Kc enciphered by storage public key:SC.Stopub.SP.K corresponding to (SP) -- that is Contents key:Kc is acquired by taking out [SC.Stopub.SP.K (Kc)] and performing decryption processing by storage private key:SC.Stopri.SP.K corresponding to SP. In addition, [A (B)] shall show the data which consist of B enciphered by A. With this gestalt, the contents decode of a user device, i.e., off-line decode, is attained as processing in a user device, without connecting with a service provider at the utilization time of contents, at i.e., the time of decode.

[0158] In addition, although the above-mentioned example explained the example of a configuration which applied the public key cryptosystem, used storage public key:SC.Stopub.SP.K corresponding to SP for encryption of a contents key, and used storage private key:SC.Stopri.SP.K corresponding to SP for decode of a contents key It is also possible to apply a common key system, and when applying a common key system, storage key (common key):SC.Sto.SP.K corresponding to SP is used for processing of the both sides of encryption of a contents key and a decryption. In this case, storage key (common key):SC.Sto.SP.K corresponding to SP is stored in the service provider management domain of a service provider where the memory of a security chip corresponds.

[0159] (b) The contents key stored in the attribute certificate set up corresponding to

the contents which offer a service provider to a user device when private key (common key system):SP.Sto.K which a service provider holds is applied : encipher with the application of private key:SP.Sto.K in which a service provider holds Kc. Even if a user device receives an attribute certificate, it cannot decode encryption contents key: [SP.Sto.K (Kc)] stored in the attribute certificate. The private key which a service provider holds: It is because SP.Sto.K does not hold the user device.

[0160] Therefore, the following processings are needed in order to use contents (decryption). First, a user device sends an attribute certificate to a service provider, performs the decode demand of a contents key, and decrypts contents key:Kc in a service provider by private key:SP.Sto.K which a service provider holds. contents key:Kc by which the user device was decrypted from the service provider -- acquiring -- this -- encryption contents are decoded by contents key:Kc. Unlike the above-mentioned gestalt of (a), with this gestalt, a user device becomes indispensable [connecting with a service provider at the utilization time of contents at i.e., the time of decode,]. That is, on-line processing is needed.

[0161] (c) The gestalt which uses this global common key when global common key:kg generated as a key shared between a system holder (SH) and a user device is applied is a configuration for setting to the service provider which performs distribution of contents, preventing that contents are distributed and used without authorization of a system holder, and performing managed contents distribution by the system holder (SH). The contents manufacturer key which the contents creator which offers contents to a service provider has, The contents distribution person key which the service provider which performs contents distribution has, And the encryption key data which performed encryption processing which combined each global common key:kg key generated as a key shared between a system holder (SH) and a user device are stored in an attribute certificate. It is the configuration which enabled it for the service provider itself to prevent taking out a contents key, and to take out contents key:Kc only in a user device by distributing to the user device which is an entity as a contents user.

[0162] Hereafter, each of these gestalten are explained to a detail. First, the issue processing sequence of the attribute certificate common to above-mentioned (a) - (c) is explained using drawing 18 .

[0163] The processing sequence of drawing 18 explains to a detail generation of the attribute certificate constituted as a part of contents purchase processing sequence of drawing 15 explained previously, and transmitting processing. A security chip is built in, the service provider management domain is generated by the memory in a security

chip, and a user device presupposes that service provider management information is storing ending.

[0164] Processing of drawing 18 is explained. As for the user device with (1) security chip, an attribute certificate (AC) is required from a service provider after materializing the mutual recognition between a user device and a service provider. A user's public key certificate (PKC) is attached to the data which signed Application ID and the use condition data which the user chose further as the user ID registered into the service provider management domain, and an assignment identifier of contents with a user's private key (private key corresponding to a service provider), and it transmits to an attribute certificate (AC) demand. Use condition data are tbe data, such as for example, a count of a contents use limit, and a use term, and when selectable, they are contained by the user as user tbe data.

[0165] Being added in order to enable verification of a data alteration, and using the above-mentioned MAC value can also be signed, and it can also apply the electronic signature using a public key cryptosystem.

[0166] The generation method of electronic signature using a public key cryptosystem is explained using drawing 19 . The processing shown in drawing 19 is the generation processing flow of the electronic signature data which used EC-DSA (Elliptic Curve Digital SignatureAlgorithm) (IEEE P1363/D3). In addition, the example which used the elliptic curve cryptosystem (Elliptic Curve Cryptosystem (hereafter referred to as ECC)) as public key encryption here is explained. in addition, in the data processor of this invention, it is also possible to use RSA cryptograph (Rivest, Shamir, Adleman), such as etc. (ANSI X9.31), in the same public key cryptosystem besides an elliptic curve cryptosystem.

[0167] Each step of drawing 19 is explained. In step S1, let the base point on an elliptic curve, and r into the order of G, and let [p / the characteristic, and a and b] Ks be a private key (0<Ks<r) for the multiplier (elliptic curve: y2=x3+ax+b, four a3+27b2!=0 (mod p)) of an elliptic curve, and G. Step S2 The hash value of Message M is calculated by setting, and it considers as f=Hash (M).

[0168] Here, how to calculate a hash value using a Hash Function is explained. A Hash Function is a function which considers a message as an input, compresses this into the data of predetermined bit length, and is outputted as a hash value. It is difficult for a Hash Function to predict an input from a hash value (output), and when 1 bit of the data inputted into the Hash Function changes, discovering different input data which many bits of a hash value change and has the same hash value has the difficult description. As a Hash Function, MD4, MD5, SHA-1, etc. may be used and DES-CBC

may be used. In this case, MAC (check value: it is equivalent to ICV) used as a final output value serves as a hash value.

[0169] Continuously, at step S3, a random number u (0<u<r) is generated and the coordinate V (Xv, Yv) which doubled the base point u by step S4 is calculated. In addition, the addition on an elliptic curve and 2 double ** are defined as follows.

[0170]

[Equation 1] When P= (Xa, Ya), Q= (Xb, Yb), and R=(Xc, Yc) =P+Q, it is Xc=lambda 2-2 XaYc=lambda x(Xa-Xc)-Yalambda=(3 (Xa) 2+a)/(2Ya) [0171] at the time (2 double **) of Xc=lambda 2-Xa-XbYc=lambda x(Xa-Xc)-Yalambda=(Yb-Ya)/(Xb-Xa)P=Q at the time of P!=Q (addition). u times of Point G are calculated using these (although a rate is slow, it carries out as follows as the most intelligible operation approach.). G, 2xG, and 4xG .. is calculated and 2 ixG (value which 2-double-**(ed) G i times (bit position when counting i from LSB of u)) corresponding to the place carries out binary number expansion of the u, and 1 stands is added.

[0172] At step S5, c=Xvmod r is calculated and it judges whether this value is set to 0 at step S6, if it is not 0, d=[(f+cKs) /u] mod r will be calculated at step S7, it judges whether d is 0 at step S8, and if d is not 0, c and d will be outputted as electronic signature data by step S9. If r is assumed to be the die length of 160 bit length, electronic signature data serve as 320 bit length.

[0173] In step S6, when c is 0, it returns to step S3 and a new random number is regenerated. Similarly, when d is 0 at step S8, it returns to step S3 and a random number is regenerated.

[0174] Next, the verification approach of electronic signature using a public key cryptosystem is explained using drawing 20 . step S11 -- M -- let the multiplier (elliptic curve: y2=x3+ax+b, four a3+27b2!=0 (mod p)) of an elliptic curve, and G as the base point on an elliptic curve, and let [a message and p / the characteristic, and a and b] the order of G, G, and KsxG be public keys (0<Ks<r) for r. It verifies whether the electronic signature data c and d fill 0<c<r and 0<d<r with step S12. When this is being filled, at step S13, the hash value of Message M is calculated and it considers as f=Hash (M). Next, h= 1-/d mod r is calculated at step S14, and it is h1=fh at step S15. mod r, h2=chmod r is calculated.

[0175] In step S16, point P=(Xp, Yp) =h1xG+h2 and KsxG are calculated using h1 and h2 which were already calculated. Since the electronic signature verification person knows the base point G and KsxG, he can do count of the scalar multiple of the point on an elliptic curve like step S4 of drawing 19 . And Point P judges whether it is an infinite point at step S17, and if it is not an infinite point, it will progress to step S18

(the judgment of an infinite point will be able to be performed at step S16 in fact.). That is, if addition of P= (X, Y) and Q= (X, -Y) is performed, lambda cannot be calculated but it will have become clear that P+Q is an infinite point. Xp mod r is calculated at step S18, and it compares with the electronic signature data c. Finally, when this value is in agreement, it progresses to step S19 and electronic signature judges with the right.

[0176] When electronic signature is judged to be the right, it turns out that data were not altered but the person holding the private key corresponding to a public key generated electronic signature.

[0177] In step S12, when the electronic signature data c or d do not fill $0<c<r$ and $0<d<r$, it progresses to step S20. Moreover, in step S17, also when Point P is an infinite point, it progresses to step S20. In step S18, also when the value of Xp mod r is not in agreement with the electronic signature data c, it progresses to step S20 further again.

[0178] In step S20, when judged with electronic signature not being right, it turns out that those who data are altered or hold the private key corresponding to a public key did not generate electronic signature. Although the alteration is possible only by taking signature attachment and a hash as mentioned above, there is effectiveness same with the ability not to alter substantially by detection.

[0179] The contents key corresponding to the contents specified with Application ID when it checks that the service provider which received the attribute certificate (AC) demand does not have an alteration in requested data by above-mentioned signature verification processing etc.: Encipher Kc. This contents key: The key applied to encryption of Kc is global common key:kg either which is generated as a key shared between storage private key:SC.Stopri.SP.K corresponding to SP stored in each service provider management domain of the security chip of the above-mentioned (a) user device, private key:SP.Sto.K which the (b) service provider holds, (c) system holder (SH), and a user device.

[0180] Furthermore, a service provider generates the attribute certificate which stores the data requirement besides use condition data of contents, and shows it to drawing 5 mentioned above. The electronic signature which used the private key of a service provider is added to the generated attribute certificate. Generation processing of electronic signature is performed according to the same processing as the processing flow of drawing 19 . The attribute certificate generated by the service provider is sent to a user device, and signature verification processing is performed in a user device according to the same sequence as the processing flow of

above-mentioned drawing 20 .

[0181] Furthermore, it is desirable for a user device to acquire the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC), and to verify a public key certificate if needed. For example, when the reliability of the publisher of an attribute certificate (AC) is uncertain, the judgment of whether to have the public key certificate of a certificate authority justly is attained by verifying the public key certificate of the publisher of an attribute certificate (AC). In addition, as the public key certificate mentioned above, when hierarchy organization is being made, it is desirable to perform to verification of the public key certificate which followed the path on the high order, and performed a chain of verification, and the root certificate authority (CA) published. In addition, this chain verification may be indispensable.

[0182] The detail of related check processing with an attribute certificate (AC) and a public key certificate (PKC) and verification processing of each certificate is explained with reference to drawing. The flow of drawing 21 is check processing of the public key certificate (PKC) relevant to the attribute certificate (AC) performed in case verification of an attribute certificate (AC) is performed.

[0183] If the attribute certificate for a check (AC) is set (S21), the public key certificate information (holder) field of AC holder of an attribute certificate will be extracted (S22). The publisher information on the public key certificate stored in the extracted public key certificate information (holder) field (PKC issuer), A public key certificate serial number (PKC serial) is checked (S23). A public key certificate (PKC) is searched based on the publisher information (PKCissuer) on a public key certificate, and a public key certificate serial number (PKC serial) (S24), and the public key certificate (PKC) related with the attribute certificate (AC) is acquired (S25).

[0184] As shown in drawing 21 , correlation is made by the public key certificate publisher information (PKC issuer) and the public key certificate serial number (PKC serial) in the public key certificate information (holder) field where the attribute certificate (AC) and the public key certificate (PKC) were stored in the attribute certificate.

[0185] Next, with reference to drawing 22 , verification processing of a public key certificate (PKC) is explained. Verification of the public key certificate (PKC) shown in drawing 22 is a chain verification processing flow which follows a certificate chain from low order to a high order, acquires the chain information to the top public key certificate, and performs signature verification of the public key certificate to the most significant (root CA). First, the public key certificate (PKC) used as the

candidate for verification is set (S31), and a public key certificate (PKC) signer is specified based on public key certificate (PKC) storing information (S32). Furthermore, it judges whether it is the top public key certificate of the certificate chain used as the candidate for verification (S33), and when it is not the most significant, the top public key certificate is acquired from direct or a repository (S34). If the top public key certificate is acquired and set (S35), a verification key (public key) required for signature verification is acquired (S36), and it judges whether the signature for verification is a self-signature (S37), and when it is not a self-signature, low order PKC will be set (S39) and signature verification will be performed based on the verification key (public key) acquired from the public key certificate of a high order (S40). In addition, in the self-signature judging in step S37, in a self-signature, verification which used the self public key as the verification key is performed (S38), and it progresses to step S41.

[0186] It judges whether when it succeeded in signature verification (S41:Yes), the verification of PKC made into the purpose was completed (S42), and PKC verification is ended when having completed. When having not completed, to step S36, acquisition of a required verification key (public key) and signature verification of a low-ranking public key certificate are repeated to return and signature verification, and it performs. In addition, when signature verification goes wrong (S41:No), it progresses to step S43 and processing of stopping the procedure of error processing, for example, after that, is performed.

[0187] Next, with reference to drawing 23 , verification processing (Example 1) of an attribute certificate (AC) is explained. First, the attribute certificate (AC) used as the candidate for verification is set (S51), and the owner and signer of an attribute certificate (AC) are specified based on the attribute (certificate AC) storing information (S52). Furthermore, the public key certificate of the owner of an attribute certificate (AC) is acquired from direct or a repository (S53), and verification processing of a public key certificate is performed (S54).

[0188] When verification of a public key certificate goes wrong (it is No at S55), it progresses to step S56 and error processing is performed. For example, subsequent processing is stopped. When it succeeds in verification of a public key certificate (it is Yes at S55), the public key certificate corresponding to the signer of an attribute certificate (AC) is acquired from direct or a repository (S57), and verification processing of a public key certificate is performed (S58). When verification of a public key certificate goes wrong (it is No at S59), it progresses to step S60 and error processing is performed. For example, subsequent processing is stopped. When it

succeeds in verification of a public key certificate (it is Yes at S59), a public key is picked out from the public key certificate corresponding to the signer of an attribute certificate (AC) (S61), and signature verification processing of an attribute certificate (AC) is performed using ** and the taken-out public key (S62). When signature verification goes wrong (it is No at S63), it progresses to step S64 and error processing is performed. For example, subsequent processing is stopped. When it succeeds in signature verification (it is Yes at S63), attribute certificate verification is ended and it shifts to subsequent processing, for example, acquisition of the encryption contents key in an attribute certificate etc.

[0189] Next, with reference to drawing 24 , verification processing (Example 2) of an attribute certificate (AC) is explained. This example is an example to which it was presupposed that the verification is omitted, when it judges whether the public key certificate which is needed for verification processing of an attribute certificate (AC) is stored and the public key certificate is stored in the self-device. First, the attribute certificate (AC) used as the candidate for verification is set (S71), and the owner and signer of an attribute certificate (AC) are specified based on the attribute (certificate AC) storing information (S72). Furthermore, the public key certificate (PKC) of the owner of an attribute certificate (AC) searches whether storing preservation is carried out in the memory in a self-device (S73). When saved (it is Yes at S74), the public key certificate of the owner of an attribute certificate (AC) is taken out (S75), and it progresses to ** and step S81.

[0190] When the public key certificate (PKC) of the owner of an attribute certificate (AC) is not saved in the memory in a self-device (it is No at S74), the public key certificate (PKC) of the owner of an attribute certificate (AC) is acquired from direct or a repository (S76), and verification processing of the public key certificate (PKC) of the owner of an attribute certificate (AC) is performed (S77). When verification of a public key certificate goes wrong (it is No at S78), it progresses to step S79 and error processing is performed. For example, subsequent processing is stopped. When it succeeds in verification of a public key certificate (it is Yes at S78), after saving the verification result of a public key certificate (S80), the public key certificate (PKC) corresponding to the signer of an attribute certificate (AC) searches whether storing preservation is carried out in the memory in a self-device (S81). When saved (it is Yes at S82), the public key certificate of the signer of an attribute certificate (AC) is taken out (S83), and it progresses to ** and step S88.

[0191] When the public key certificate (PKC) of the signer of an attribute certificate (AC) is not saved in the memory in a self-device (it is No at S82), the public key

certificate (PKC) of the signer of an attribute certificate (AC) is acquired from direct or a repository (S84), and verification processing of the public key certificate (PKC) of the signer of an attribute certificate (AC) is performed (S85). When verification of a public key certificate goes wrong (it is No at S86), it progresses to step S87 and error processing is performed. For example, subsequent processing is stopped. When it succeeds in verification of a public key certificate (it is Yes at S86), the key (public key) applied to signature verification of a public key certificate to an attribute certificate (AC) is taken out (S88), and signature verification processing of an attribute certificate (AC) is performed (S89). When signature verification goes wrong (it is No at S90), it progresses to step S91 and error processing is performed. For example, subsequent processing is stopped. When it succeeds in signature verification (it is Yes at S90), attribute certificate verification is ended and it shifts to subsequent processing, for example, acquisition of the encryption contents key in an attribute certificate etc.

[0192] When verification of the attribute certificate by the user device is made, an attribute certificate will be stored in the memory of the security chip in a user device, or the external memory under management of the user device control section besides a security chip, and will perform acquisition of the encryption contents key in an attribute certificate, and decryption processing to the utilization time of contents. The processing which acquires and decodes the contents key enciphered from the attribute certificate is explained below.

[0193] (a) storage public key: corresponding to (the service provider SP) corresponding to the storage private key corresponding to SP -- the service provider corresponding to [when SC.Stopub.SP.K is applied] the storage private key corresponding to (a) SP of the above-mentioned first -- apply storage public key:SC.Stopub.SP.K corresponding to (SP) to encryption of contents key:Kc, and explain the contents use processing based on the attribute certificate which stored [SC.Stopub.SP.K (Kc)].

[0194] The storage private key corresponding to SP: SC.Stopri.SP.K is stored in a service provider management domain, and a user can take out and use this key by the authentication information (password) input mentioned above. Therefore, a contents key: Kc can be acquired as off-line processing, without connecting with a service provider, and the decode of contents of it is attained.

[0195] Drawing which explains the sequence of the encryption contents key acquisition from an attribute certificate, decode, and the contents decryption processing with a contents key to drawing 25 is shown.

[0196] It explains according to the sequence diagram of drawing 25 . Drawing 25 shows processing of the memory inside a security chip, a security chip control section, and a user device control section from the left. First, the application ID as contents identification information which the user inputted to the user device is transmitted to a security chip control section, and the attribute certificate (AC) corresponding to Application ID is acquired from memory. It verifies whether it is an attribute certificate corresponding to Application ID, an attribute certificate is set to a security chip control section, and a user device requires acquisition (decode) processing of contents key:Kc.

[0197] A security chip control section performs signature verification of an attribute certificate, it checks that there is no data alteration, takes out encryption contents key: [SC.Stopub.SP.K (Kc)] stored in the attribute certificate, performs decryption processing with the application of storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain, and acquires contents key:Kc. Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section.

[0198] Next, a user device control section acquires the encryption contents which should be decoded with the application of the acquired contents key from memory through a security chip control section. When encryption contents are stored in external memory (for example, hard disk) instead of memory etc. in a security chip, encryption contents are acquired from external memory. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security chip is performed, and the contents obtained as a decryption processing result are outputted to a user device control section.

[0199] In addition, although considered as the configuration which applied the public key cryptosystem, used storage public key:SC.Stopub.SP.K corresponding to SP for encryption of a contents key, and used storage private key:SC.Stopri.SP.K corresponding to SP for decode of an encryption contents key in the above-mentioned example of a configuration It is also possible to apply a common key system, and when applying a common key system, storage key (common key):SC.Sto.SP.K corresponding to SP is used for processing of the both sides of encryption of a contents key and a decryption. In this case, storage key (common key):SC.Sto.SP.K corresponding to SP is stored in the service provider management domain of a service provider where the memory of a security chip corresponds.

[0200] (b) a service provider -- holding -- a private key (common key system) -- : -- SP . -- Sto . -- K -- having applied -- a case -- next -- the above-mentioned -- (-- b --) -- a service provider -- holding -- a private key -- : -- SP . -- Sto . -- K -- contents -- a key -- : -- Kc -- encryption -- applying -- [-- SP . -- Sto . -- K -- (-- Kc --) --] -- having stored -- an attribute -- a certificate -- being based -- contents -- use -- processing -- ******** -- explaining .

[0201] The private key which a service provider holds: SP.Sto.K is a key which a service provider holds and is not stored in the user device. Therefore, in order for a user device to acquire contents key:Kc, it will connect with a service provider, it will be necessary to require decryption processing of a contents key from a service provider, and the contents decode by on-line processing will be performed.

[0202] Drawing which explains the sequence of the contents key acquisition from an attribute certificate, decode, and the contents decryption processing with a contents key to drawing 26 is shown.

[0203] It explains according to the sequence diagram of drawing 26 . Drawing 26 shows the processing in the memory inside a security chip, a security chip control section, a user device control section, and a service provider from the left.

[0204] First, the application ID as contents identification information which the user inputted to the user device is transmitted to a security chip control section, and the attribute certificate (AC) corresponding to Application ID is acquired from memory. It verifies whether it is an attribute certificate corresponding to Application ID, an attribute certificate is set to a security chip control section, and a user device requires acquisition (decode) processing of contents key:Kc.

[0205] It connects through a user device after verification of an attribute certificate to the service provider which is attribute certificate issue-origin, and a security chip control section performs mutual recognition processing between a security chip and a service provider. This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a security chip and a service provider share a session key (Kses).

[0206] If mutual recognition is materialized, the control section of a security chip will send an attribute certificate to a service provider. The data of the contents key enciphered by private key:SP.Sto.K which a service provider holds, i.e., [SP.Sto.K],

(Kc) are stored in the attribute certificate.

[0207] The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. By these verification processings, if the justification of an attribute certificate is checked, using private key:SP.Sto.K which self owns, a service provider will perform decryption processing of encryption contents key: [SP.Sto.K (Kc)] stored in the attribute certificate, and will take out contents key:Kc. Furthermore, the taken-out contents key: Encipher by the session key (Kses) which generated Kc in previous mutual recognition processing, and transmit to the security chip of a user device.

[0208] If the contents key enciphered by the session key from the service provider, i.e., [Kses], (Kc) is received, the control section of a security chip will perform decryption processing using the session key held at the time of mutual recognition, and will acquire contents key:Kc.

[0209] Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section. Next, a user device control section acquires the encryption contents which should be decoded with the application of the acquired contents key from memory through a security chip control section. When encryption contents are stored in external memory (for example, hard disk) instead of memory etc. in a security chip, encryption contents are acquired from external memory. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security chip is performed, and the contents obtained as a decryption processing result are outputted to a user device control section.

[0210] (c) When global common key:kg generated as a key shared between a system holder (SH) and a user device is applied next, explain to encryption of contents key:Kc processing stored in an attribute certificate indirectly with the application of global common key:kg generated as a key shared between a system holder (SH) and a user device. The gestalt using this global common key is enabled to take out contents key:Kc only in a user device, and the service provider which performs distribution of contents is making ejection of a contents key impossible, it prevents that contents are distributed and used without authorization of a system holder, and it becomes possible to perform managed contents distribution by the system holder (SH).

[0211] The encryption key data which performed encryption processing which combined each global common key:kg key generated as the contents manufacturer key which the contents creator which offers contents to a service provider specifically has, the contents distribution person key which the service provider which performs contents distribution has, and a key shared between a system holder (SH) and a user device are stored in an attribute certificate.
[0212] Drawing explaining the detail of the processing which stores and distributes the encryption data of contents key:Kc to encryption of contents key:Kc indirectly with the application of global common key:kg at drawing 27 at an attribute certificate is shown.
[0213] The system holder 301 which builds the platform of contents distribution and is managed, the service provider (CD: contents distributor) 302 which performs contents distribution, and contents are generated or managed in drawing 27 , and the user device 304 as an end entity which receives contents is shown in it from the contents creator 303 which offers encryption contents to a service provider 302, and the service provider 302. In addition, the user device 304 has a security chip like the example of the above-mentioned (a) and (b), and the service provider management domain is generated by the memory area in a security chip.
[0214] Processing of drawing 27 is explained. First, the contents key which the contents creator 303 generated key:Kc for enciphering the contents used as the candidate for distribution with the random number, and was generated (common key system): Using Kc, encipher (1) contents and provide for a service provider 302.
[0215] Furthermore, the service-provider key which the system holder 301 receives contents creator key (common key system):Kcc which (2) contents creator 303 to the contents creator 303 holds, and the (3) service provider (CD: contents distributor) 302 to the service provider 302 holds (common key system): Receive Kcd. In addition, these keys may deliver in advance.
[0216] The system holder 301 enciphers contents creator key:Kcc by service provider key:Kcd, and enciphers this encryption data by global common key:kg further. namely, encryption key data: [Kg ([Kcd (Kcc)])] -- generating -- (4) -- this is sent to the contents creator 303. In addition, [Kg ([Kcd (Kcc)])] may deliver in advance. Global common key: kg is a key which the user device 304 shares with the system holder 301. the user device 304 -- the time of (5) device manufacture -- the time of device sale -- or -- at least -- by [before purchase initiation of contents] -- one or more -- global -- common -- key:kg1-Kgn is stored and, as for these, an update process is performed under management of a system holder. About an update process, it

mentions later.
[0217] data: [Kcc (Kc)] as which the contents creator 303 enciphered contents key:Kc by contents creator key:Kcc -- generating -- (6), while transmitting this to a service provider 302 The contents creator key received from the system holder 301 : Kcc is enciphered by service provider key:Kcd. Furthermore, encryption key data: [Kg ([Kcd (Kcc)])] which enciphered this encryption data by global common key:kg is transmitted to a service provider 302. In addition, [Kg ([Kcd (Kcc)])] may deliver in advance.
[0218] If the user device 304 performs (7) contents purchase demand to a service provider 302, (8) service providers will generate the attribute certificate corresponding to demand contents, and will transmit to the user device 304. The data which enciphered cryptographic-key data [above-mentioned]: [Kg ([Kcd (Kcc)])], i.e., contents creator key:Kcc, by service-provider key:Kcd in the attribute certificate (AC) to generate, and enciphered this encryption data by global common key:kg further in it, and a contents key: Data: [Kcc (Kc)] which enciphered Kc by contents creator key:Kcc is stored. In addition, data, such as use conditions of contents, are stored, the electronic signature of a service provider 302 is made, and it is transmitted to the user device 304. The user device 304 stores the received attribute certificate (AC) in memory.
[0219] (10) after the user device 304 carries out (9) mutual recognition to the utilization time of contents between service providers 302 -- an attribute certificate [finishing / reception / previously] (AC) is transmitted to a service provider 302. Mutual recognition processing is performed as mutual recognition processing between the security chip of a user device, and a service provider. This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a security chip and a service provider share a session key (Kses).
[0220] Data: [Kg ([Kcd (Kcc)])] which enciphered the above-mentioned contents creator key:Kcc by service-provider key:Kcd in the attribute certificate, and enciphered this encryption data by global common key:kg further in it, and a contents key: Data: [Kcc (Kc)] which enciphered Kc by contents creator key:Kcc is stored.
[0221] The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it

is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. The service-provider key in which self owns (11) service providers by these verification processings if the justification of an attribute certificate is checked: Encipher Kcd by session key:Kses generated at the time of mutual recognition, generate encryption key data [Kses (Kcd)], and transmit this to a user device.

[0222] About the encryption key data [Kses (Kcd)] received from the (12) service provider 302, the security chip control section of the user device 304 performs decryption processing which used the session key, and acquires service provider key:Kcd. In addition, a service-provider key: Kcd may be kept to a service provider memory area in advance.

[0223] Next, the security chip control section of the user device 304 enciphers contents creator key:Kcc (13) attribute certification in the letter by service provider key:Kcd, further, about data: [Kg ([Kcd (Kcc)])] which enciphered this encryption data by global common key:kg, is decoded by global common key:kg which self owns, and acquires [Kcd (Kcc)] first. Furthermore, the service-provider key acquired by the decode of encryption key data which received from the (14) service provider 302: Acquire contents creator key:Kcc by decryption processing which applied Kcd.

[0224] Furthermore, the contents creator key which the security chip control section of (15) user device 304 took out data: [Kcc (Kc)] which enciphered contents key:Kc attribute certification in the letter by contents creator key:Kcc, and was acquired by said processing: Perform decryption processing which applied Kcc and acquire contents key:Kc.

[0225] Contents key: If it succeeds in acquisition of Kc, the security chip control section of the user device 304 will notify that decode preparation of contents was completed to a user device control section.

[0226] The user device 304 transmits the encryption contents ((16) processings) acquired from the service provider 302 to a security chip, and performs decryption processing which applied contents key:Kc to encryption contents within the security chip.

[0227] In addition, it is desirable to perform mutual recognition among entities which perform data transmission and reception before data transmission and reception, such as a key between each above-mentioned entity and an encryption key, and to perform the data transmission and reception on condition of authentication formation, and it is desirable to consider as the configuration which enciphered the transmitted and

received data by the session key, and gave the signature.
[0228] Thus, only a user device and a system holder own a global common key, and other entities do not hold and consist of other entities as an unacquirable key. Therefore, also in a service provider, acquisition of a contents key is impossible and prevention of circulation of a contents key without authorization of a system holder and circulation of contents is attained.
[0229] A global common key is updated if needed. The support center under management of a system holder performs updating. The global common key update process sequence performed between a support center and a user device is shown in drawing 28 . Two global common keys Kg1 and Kg2 shall be stored in the memory area in the security chip of a user device. The key data encryption in an attribute certificate is made using these either, and decryption processing is performed. Or it is good also as a configuration which performs the key data encryption in an attribute certificate using two keys, for example with the application of a Triple DES algorithm, and performs decryption processing using two keys.
[0230] Each processing shown in the processing sequence of drawing 28 is explained. Drawing 28 shows the processing in the support center which is from the left under management of a security chip control section, a user device control section, and a system holder.
[0231] first, a user device control section is global -- common -- if the renewal demand of key:kg is transmitted to a security chip control section, it will connect through a user device to the support center under management of a system holder, and a security chip control section will perform mutual recognition processing between a security chip and a support center. This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a security chip and a support center share a session key (Kses).
[0232] when mutual recognition is materialized, the control section of a security chip is global to a support center -- common -- the renewal demand of key:kg is outputted. the object [finishing / a support center / generation / already] for updating -- global -- common -- it generated according to key:kg3 or a demand -- global -- common -- it enciphers by session key:Kses which generated key:kg3 in authentication processing, and encryption key data: [Kses (kg3)] is transmitted to the security chip

of a user device.
[0233] the control section of a security chip was enciphered by the session key from the support center -- global -- common -- global [perform decryption processing using the session key held at the time of mutual recognition and], when key:kg3 (kg3), i.e., [Kses], are received -- common -- key:kg3 are acquired.
[0234] global -- common -- when it succeeds in acquisition of key:kg3, a security chip control section is global -- common -- key:kg1 was acquired -- global -- common -- it transposes to key:kg3. Thereby, the global common key which a user device holds is set to Kg2 and Kg3. Since the global common key which a user device holds is meaningful also including the order relation, it also combines the order relation of [Kg1, Kg2], and is corrected with [Kg2, Kg3]. With key data, a global common key shall also double the order relation currently held within the user device, and shall hold data.
[0235] Drawing 29 is drawing having shown the example of a processing sequence which a service provider intercedes and performs renewal of a global common key, without a user device and a support center performing immediate-data transmission and reception.
[0236] Each processing shown in the processing sequence of drawing 29 is explained. Drawing 29 shows the processing in the support center which is from the left under management of a security chip control section, a user device control section, a service provider, and a system holder.
[0237] it is updated in a support center -- new -- global -- common -- key:kg3 are generated in advance and global -- common -- finishing [3 / key:kg/ distribution to a user device] already -- global -- common -- it enciphers by key:kg2 and data: [Kg2 (kg3)] is generated, and a signature is given to this by private key:Kss of a support center, and it sends to it at a service provider. A service provider has data [Kg2 (kg3)] and Sig [Kss]. In addition, A and Sig [B] shall show the data configuration which added the signature with Key B to Data A.
[0238] next, a user device control section is global -- common -- if the renewal demand of key:kg is transmitted to a security chip control section, it will connect through a user device to a service provider, and a security chip control section will perform mutual recognition processing between a security chip and a service provider. This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a

security chip and a service provider share a session key (Kses).
[0239] when mutual recognition is materialized, the control section of a security chip is global to a service provider -- common -- the renewal demand of key:kg is outputted. A service provider transmits data [finishing / reception] [Kg2 (kg3)] and Sig [SuC] from a support center to the security chip of a user device.
[0240] If a transfer of the data [Kg2 (kg3)] from [from a service provider] a support center and Sig [SuC] is received, the control section of a security chip As opposed to key:kg3 [2 (kg3)], i.e., [Kg], signature verification processing is performed, and self owns, after checking that there is no data alteration -- global -- common -- it was enciphered by key:kg2 -- global -- common -- global -- common -- global [perform decryption processing using key:kg2 and] -- common -- key:kg3 are acquired. In addition, when applying the public key of a support center to signature verification of a support center, the public key certificate of a support center is transmitted with data [Kg2 (kg3)] and Sig [SuC] to a user device, or it distributes to the user device beforehand.
[0241] global -- common -- when it succeeds in acquisition of key:kg3, a security chip control section is [in the key storing field of memory, for example, the above-mentioned device management domain] global -- common -- global to a key:kg1 write-in field -- common -- key:kg3 are overwritten. The global common key which a user device holds is updated by this update process two, Kg2 and Kg3.
[0242] If [decryption processing using decoder] encryption contents or an encryption contents key is the configuration which makes a decoder with the decryption processing facility of dedication perform processing, it will become accelerable [processing]. However, since a decoder has the hard configuration which became independent of a security chip, it is necessary to perform the contents key within a decoder, and a decryption of contents, after checking the dependability of a decoder. Hereafter, decryption processing of the encryption contents using a decoder or an encryption contents key is explained with reference to drawing.
[0243] Drawing explaining a security chip, the contents key in the case of having a decoder, and the decryption processing sequence of contents is shown in a user device at drawing 30 .
[0244] A user device has the security chip 210, the memory section 222 which consists of a decoder 280, a hard disk, a flash memory, etc., and the user device side control section 221 which performs data I/O and various processing run commands to the security chip 210, and a decoder 280 and the memory section 222 with high order software.

[0245] The sequence at the time of contents decryption processing is explained. First, if the contents use demand which specified contents is inputted into the user device side control section 221 by actuation of the input means by the user, the user device side control section 221 will search the attribute certificate (AC) corresponding to the assignment contents stored in the memory section 222. The attribute certificate (AC) extracted by retrieval is transmitted to the security chip 210, and verification processing of an attribute certificate (AC) is performed within the security chip 210.
[0246] If it succeeds in the attribute (certificate AC) verification processing, share processing of mutual recognition and a session key will be performed between the security chip 210 and a decoder 280. After the security chip 210 after mutual recognition is materialized decrypts the encryption contents key picked out from the attribute certificate (AC), it re-enciphers a contents key using the session key shared with the decoder 280 at the time of mutual recognition, and transmits it to a decoder 280. The decoder 280 which received the encryption contents key performs a decryption of an encryption contents key with the application of a session key, and acquires a contents key.
[0247] Next, the user device side control section 221 searches and takes out the encryption contents stored in the memory section 222, and transmits to a decoder 280. A decoder 280 performs decryption processing with the application of the contents key which acquired the inputted encryption contents previously.
[0248] In the processing which applied the decoder mentioned above, a contents key is not used within the security chip 210. Moreover, a decoder decrypts encryption contents and carries out the external output of voice or the image data as analog output. In addition, only when ID and the authentication method of a decoder to attest may be described, and it judges whether the security chip 210 suits the decoder ID the decoder was described to be by the attribute certificate (AC) at the time of mutual recognition, and an authentication method in an attribute certificate (AC) in this case and suits it, a contents key is outputted to a decoder.
[0249] The processing sequence using a decoder is explained using drawing 31 . In drawing 31 , each processing of a security chip, high order software (user device side control section), and a decoder is shown from the left.
[0250] If the contents use demand which specified contents is inputted into high order software (user device side control section) by actuation of the input means by the user, high order software (user device side control section) will acquire the application ID corresponding to assignment contents, and the attribute certificate (AC) corresponding to the application ID stored in memory, such as a hard disk, will be

searched based on Application ID.

[0251] If it is transmitted to a security chip with the attribute (certificate AC) verification processing instruction, a security chip performs verification processing of an attribute certificate (AC) and the attribute certificate (AC) extracted by retrieval succeeds in the attribute (certificate AC) verification processing, it will output a response message to high order software (user device side control section) while a security chip picks out an encryption contents key from an attribute certificate (AC) and it performs decryption processing.

[0252] Next, share processing of mutual recognition and a session key is performed through high order software (user device side control section) between a security chip and a decoder. After the security chip after mutual recognition is materialized decrypts the encryption contents key picked out from the attribute certificate (AC), it re-enciphers a contents key using the session key shared with the decoder at the time of mutual recognition, and transmits it to a decoder. The decoder which received the encryption contents key performs a decryption of an encryption contents key with the application of a session key, and acquires a contents key.

[0253] Next, a user device side control section searches and takes out the encryption contents stored in memory, and transmits to a decoder. A decoder performs decryption processing with the application of the contents key which acquired the inputted encryption contents previously.

[0254] Next, the contents decryption processing using a decoder is explained with reference to the flow of drawing 32 .

[0255] If the contents use demand which specified contents is inputted into high order software (user device side control section) by actuation of the input means by the user in step S101, it will set to step S102. High order software (user device side control section) acquires the application ID corresponding to assignment contents, and sets it to step S103. Based on Application ID, the attribute certificate (AC) corresponding to the application ID stored in memory, such as a hard disk, is searched. In step S104, the attribute certificate (AC) extracted by retrieval is transmitted to a security chip with the attribute (certificate AC) verification processing instruction, and if a security chip performs verification processing of an attribute certificate (AC) in step S105 and it succeeds in the attribute (certificate AC) verification processing, a security chip will pick out an encryption contents key from an attribute certificate (AC), and it will perform decryption processing. Moreover, in step S106, a response message is outputted to high order software (user device side control section).

[0256] Subsequent processing is stopped when it does not succeed in the attribute

(certificate AC) verification processing. In a verification success, share processing of mutual recognition and a session key is performed through high order software (user device side control section) between a security chip and a decoder. In step S108, the 1st authentication command is specifically published by the security chip from high order software (user device side control section). In step S109, high order software (user device side control section) receives the response from a security chip, and it sets to step S110 further. The 2nd authentication command is published by the decoder from high order software (user device side control section). In step S111, high order software (user device side control section) receives the response from a decoder, and it sets to step S112 further. The 3rd authentication command is published by the security chip from high order software (user device side control section). By processing whose high order software (user device side control section) receives the response from a security chip in step S113, authentication processing of the decoder by the security chip is performed. When authentication processing goes wrong (it is NG at S114), subsequent processing is stopped, and when it succeeds, it progresses to step S115.

[0257] In step S115, from high order software (user device side control section), the 4th authentication command is published by the decoder and high order software (user device side control section) receives the response from a decoder in step S116. By this processing, the success or failure of authentication of the security chip by the decoder are judged. When authentication processing is failure (it is NG at S117), subsequent processing is stopped, and when it succeeds, it progresses to step S118.

[0258] In step S118, after a security chip decrypts the encryption contents key picked out from the attribute certificate (AC), it carries out re-encryption (S118) of the contents key using the session key shared with the decoder at the time of mutual recognition, and is transmitted to high order software (user device side control section) (S119). High order software (user device side control section) transmits the received encryption contents key to a decoder (S120).

[0259] The decoder which received the encryption contents key performs a decryption of an encryption contents key with the application of a session key, and acquires a contents key (S121). High order software (user device side control section) searches and (S122) takes out the encryption contents stored in memory, and transmits them to a decoder (S123). A decoder performs decryption processing with the application of the contents key which acquired the inputted encryption contents previously (S124).

[0260] Thus, in the decryption processing using a decoder, since the contents key

which mutual recognition between a security chip and a decoder was performed, and was enciphered with the session key the condition [formation of mutual recognition] considered as the configuration outputted to a decoder, decode is performed only in the device trusted and just contents use can be secured.

[0261] As explained to the [use limit of contents] place, various use conditions, such as a count of a use limit of the contents which a service provider offers, and a use term, are included in the contents use condition related information stored in attribute information field attribute certification in the letter [corresponding to the contents which stored the use limit information on contents]. That is, they are the following information. Conditions: The count of available in the count limit of count of expiration date information use limit: in the case of information expiration date:time limitation which shows [online use contents, off-line use contents, and] any of buying-up contents, time limitation contents, the count limit contents of online, and the count limit contents of off-line they are further [0262] As for the attribute certificate corresponding to the contents which buy up and carry out contents and make contents use after buying up free, the above-mentioned conditions are set up as buying up. The above-mentioned conditions are set up as time limitation, and, as for the attribute certificate corresponding to the contents which set up the use period, an expiration date is set up. The above-mentioned conditions are set up as a count limit, and, as for the attribute certificate corresponding to the contents which set up the count limit of use, the set point (count value) is set as the count of a use limit. In addition, in count limit processing, after carrying out count verification to the count limit of off-line of managing the count of available within a user device, and performing contents use, in a service provider, there is a count limit of online of permitting the contents use within the predetermined number recorded on the attribute certificate. Moreover, there is also a combination limit mode accompanied by both limits of time limitation and a count limit. In a user device, contents are used according to these modes recorded on the attribute certificate. These concrete processing modes are explained hereafter.

[0263] In order to use contents in a user device, it is necessary to take out an encryption contents key from the attribute certification in the letter corresponding to the contents used as the candidate for use, to perform decryption processing, and to acquire contents key:Kc. It is as having stated previously that there are off-line processing performed within the security chip of a device and on-line processing which sends an attribute certificate to a service provider and requests decode in acquisition processing of this contents key. Also in contents use processing in which

the use conditions of the contents indicated by the attribute certificate were followed, off-line processing which checks use conditions within a user device, and on-line processing which needs the check by the service provider occur. According to the publication of the attribute information field of an attribute certificate, it determines which [these] are applied.

[0264] The use processing flow of the attribute certificate (AC) performed by drawing 33 with the user device in contents utilization time is shown. Each step of a processing flow is explained.

[0265] A user device will perform format check processing of an attribute certificate first, if the attribute certificate corresponding to the contents for use is chosen based on Application ID (contents identification information) (S201). A need matter is recorded on an attribute certificate and it is whether the expiration date of a certificate is effective. If format check processing ends, signature verification will be performed in step S202. As explained also in advance, an attribute certificate publisher's (for example, service provider) electronic signature is added to the attribute certificate, and a user device picks out a public key from an attribute certificate publisher's public key certificate, and performs signature verification processing (refer to drawing 20). In addition, it is desirable to also perform verification of the public key certificate used in this case and verification processing of a connective public key certificate if needed. In addition, this chain verification may be indispensable.

[0266] In the signature verification processing process of step S202, verification is materialized, and when judged with there being no alteration in an attribute certificate, it progresses to step S203. On the other hand, when verification is un-materialized and is judged by the attribute certificate in the signature verification processing process of step S202 to be those with an alteration, it progresses to step S205, and processing which applied the attribute certificate is not performed, but it is stopped, subsequent processings, i.e., contents use processing.

[0267] If it is judged with there being no alteration in an attribute certificate and progresses to step S203, the contents use condition information in the attribute information field in an attribute certificate will be acquired. That is, it is [online use contents, off-line use contents, and] any of buying-up contents, time limitation contents, the count limit contents of online, and the count limit contents of off-line to be further. According to this condition, when it is on-line processing of step S204 or is off-line, it is judged [buying up and] in step S206 whether it is a count limit.

[0268] In step S204, if judged with it being online use, with having explained using

drawing 26 previously, similarly, an attribute certificate will be sent to a service provider and verification of the use limit information in an attribute certificate will be performed. In the case of on-line processing, it is either time limitation or a count limit, and a service provider performs processing which acquires such contents use condition information from an attribute certificate, and will enable acquisition of a contents key if it is the contents use claim in a use limit. If it is the contents use claim beyond a use limit, processing which enables acquisition of a contents key will not be performed, but the message for which contents use is improper will be transmitted to a user device.

[0269] moreover, when it is judged with it being off-line use in step S204 and is judged with it buying up at step S206 and their being contents In an attribute certificate Contents key data enciphered by storage public key:SC.Stopub.SP.K corresponding to (a service provider SP) corresponding to the storage private key corresponding to SP stored in the service provider management domain of the security chip of a user device : [SC.Stopub.SP.K (Kc)] is stored. In a user device Decryption processing is performed using storage private key SC.Stopri.SP.K corresponding to SP stored in the service provider management domain, contents key:Kc is acquired, and contents are used by decode of contents.

[0270] furthermore, when it is judged with it being off-line use in step S204 and is judged with their being the contents of a count limit at step S206 Within a user device, count management is performed based on the setups of an attribute certificate. After performing the propriety judging of contents use, an update process of the count management data of contents use which performs decryption processing of the encryption contents key stored in the attribute certificate the condition [acquisition of the judgment result that use is possible], and is managed within a device etc. is performed. For this reason, it is necessary to have the management data of the count of contents use in a device.

[0271] Import processing of the count management data of use of step S207 is management data generation processing of the count of contents use. In addition, import processing of the count management data of use is performed based on an attribute certificate. There are a mode which manages the count of contents available with the security chip in a user device, and two modes which carry out storing management of the count management file at the external memory besides a security chip (for example, hard disk), and store only the hash value of management data in the memory in a security chip as management mode of the count of contents use. About these details, it mentions later. The attribute certificate application completion

message generation step of step S208 is processing which notifies from a security chip that import processing of the above-mentioned count management data of use of S207 was completed to the user device besides a security chip.

[0272] The following distinguishes hereafter the contents use conditions indicated by the attribute certificate (AC) like 4 voice, and it explains one by one.

(A) the count limit contents of online-use time limitation (contents B) online-use -- the count limit contents of (C) off-line-buying-up (contents D) off-line-use [0273] (A) The contents use conditions recorded on online-use time limitation contents **** and an attribute certificate are on-line processing, and explain processing from acquisition of the attribute certificate in the case of being the contents to which the use period was restricted to contents acquisition according to the sequence diagram of drawing 34 .

[0274] The processing sequence shown in drawing 34 has already shown the processing in the user device which is receipt ending about encryption contents, and is receipt ending about the attribute certificate which stored the use conditions corresponding to contents, and an encryption contents key from the service provider, and shows processing of the security chip control section in a user device, a user device control section (high order software), and a service provider from the left.

[0275] In drawing 34 , the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in the internal memory of a security chip, and (b) the maximum upper case (a) The service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in accessible memory at control of the external memory of a security chip, i.e., a user device control-section independent, is shown. These (a) and (b) are alternatively performed according to the storing location of an attribute certificate. Mutual recognition processing of (c) and contents acquisition processing of (d) are performed in common.

[0276] First, it explains from processing of (a). (a1) A user device control section requires retrieval of the attribute certificate corresponding to the contents for use of a security chip control section. (a2) A security chip control section outputs the list of attribute certificates [finishing / storing in the memory of a chip] to a user device control section, and displays a list by the attached browser in a user (a3) device. (a4) A user specifies the attribute certificate (AC) corresponding to use schedule contents from the displayed list, and transmits a read-out instruction to a security chip control section. (a5) A security chip control section reads the specified attribute certificate from an internal memory, outputs it to a user device control section, in a user (a6)

device, displays an attribute certificate by the attached browser, and acquires the service provider identifier in attribute certificate storing data (SP ID).

[0277] It becomes processing of (b) when the attribute certificate is stored in accessible memory by control of the external memory of a security chip, i.e., a user device control-section independent. (b1) A user device control section performs a search of the attribute certificate corresponding to the contents for use, in a user (b2) device, from AC list displayed by the attached browser, it specifies the attribute certificate (AC) corresponding to use schedule contents, is beginning to read it (b3), displays an attribute certificate, and acquires the service provider identifier (SP ID) in attribute (b4) certificate storing data.

[0278] The service provider identifier (SP ID) acquired by either processing of the above (a) and (b) is used in order to acquire information required for mutual recognition from a service provider management domain. As mentioned above, the password input set up for every service provider is required for access to a service provider management domain, and by the password input corresponding to the service provider identifier (SP ID) acquired from the attribute certificate, a user performs access to a service provider management domain, and performs mutual recognition processing between the security chip shown in (c1) of drawing 34 , and a service provider.

[0279] This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a security chip and a support center share a session key (Kses). Formation of mutual recognition performs [next] the processing shown in drawing 34 (d), i.e., contents acquisition processing.

[0280] (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the contents use demand which applied the attribute certificate to a security chip. The contents use conditions recorded on the attribute certificate in this example are online time limitation.

[0281] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in

verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example.

[0282] Furthermore, it is desirable for the control section of a security chip to acquire the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC), and to verify a public key certificate if needed. For example, when the reliability of the publisher of an attribute certificate (AC) is uncertain, the judgment of whether to have the public key certificate of a certificate authority justly is attained by verifying the public key certificate of the publisher of an attribute certificate (AC). In addition, as the public key certificate mentioned above, when hierarchy organization is being made, it is desirable to perform to verification of the public key certificate which followed the path on the high order, and performed a chain of verification, and the root certificate authority (CA) published. In addition, this chain verification may be indispensable.

[0283] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, by it, the control section of a security chip will send an attribute certificate to a service provider. It is recorded on an attribute certificate that they are online time limitation contents as use conditions, and expiration date data are stored in it. Furthermore, the data of the contents key enciphered by private key:SP.Sto.K which a service provider holds, i.e., [SP.Sto.K], (Kc) are stored.

[0284] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. By these verification processings, a check of the justification of an attribute certificate checks the use condition data and expiration date data which were stored in the attribute certificate. The contents key which will be applied to decode of the contents stored in an attribute certification in the letter if judged with it being the contents use demand within the expiration date as use conditions currently recorded on the attribute certificate: Perform decode of encryption data [of Kc]: [SP.Sto.K (Kc)].

[0285] A service provider performs decryption processing of encryption contents key: [SP.Sto.K (Kc)] stored in the attribute certificate using private key:SP.Sto.K which self owns, and takes out contents key:Kc. Furthermore, the taken-out contents key: Encipher by the session key (Kses) which generated Kc in previous mutual recognition

processing, and transmit to the security chip of a user device.

[0286] (d5) If the contents key enciphered by the session key from the service provider, i.e., [Kses], (Kc) is received, the control section of a security chip will perform decryption processing using the session key held at the time of mutual recognition, and will acquire contents key:Kc. Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section.

[0287] (d6) Next, a user device control section acquires the encryption contents [Kc (Content)] which should be decoded with the application of the acquired contents key from the memory in a security chip through the memory (for example, hard disk) or the security chip control section in a user device. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security (d7) chip is performed, the contents obtained as a decryption processing result are outputted to a user device control section, and a user (d8) device acquires contents. The contents key which acquired the control section of a security (d9) chip by decryption processing after these processings were completed: Cancel Kc and contents (Content).

[0288] Check processing of the use period based on the attribute certificate (AC) by the service provider is performed by these processings. Only when it is within the restricted use period, in a security chip, in the condition which can be decoded, it is re-enciphered and contents key:Kc is sent. Decode of contents with the contents key which the contents key was acquired in the security chip and acquired is performed, and contents use is attained in a user device.

[0289] In addition, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand.

[0290] (B) The count limit contents of online-use, next the contents use conditions recorded on the attribute certificate are on-line processing, and explain processing from acquisition of the attribute certificate in the case of being the contents to which the count of use was restricted to contents acquisition according to the sequence diagram of drawing 35 .

[0291] The processing sequence shown in drawing 35 has already shown the processing in the user device which is receipt ending about encryption contents, and is receipt ending about the attribute certificate which stored the use conditions corresponding to contents, and an encryption contents key from the service provider like the processing sequence of drawing 34 explained previously, and shows processing of the security chip control section in a user device, a user device control section (high order software), and a service provider from the left.

[0292] The service provider ID acquisition processing from an attribute certificate in case, as for the maximum upper case (a), the attribute certificate is stored in the internal memory of a security chip during the processing shown in drawing 35 , (b) shows the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in accessible memory at control of the external memory of a security chip, i.e., a user device control-section independent. These (a) and (b) are alternatively performed according to the storing location of an attribute certificate. Since each processing of (a) and (b) and mutual recognition processing of (c) are the same as the processing in the case of the online time limitation explained with reference to drawing 34 , explanation is omitted. Formation of the mutual recognition of (c) performs [next] the processing shown in drawing 35 (d), i.e., contents acquisition processing.

[0293] (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the contents use demand which applied the attribute certificate to a security chip. The contents use conditions recorded on the attribute certificate in this example are the count limits of online.

[0294] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. As for the control section of a security chip, in this verification processing, it is desirable to perform to verification of the public key certificate which followed on the high order, and performed a chain of verification, and the root certificate authority (CA) published from the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC). In addition, this chain verification may be indispensable.

[0295] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, by it, the control section of a security chip will send an attribute certificate to a service provider. It is recorded on an attribute certificate that they are the count limit contents of online as use conditions, and the count of a use limit is stored in it. Furthermore, the data of the contents key enciphered by private key:SP.Sto.K which a service provider holds, i.e., [SP.Sto.K], (Kc) are stored.

[0296] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. By these verification processings, a check of the justification of an attribute certificate checks the use condition data and the count of a use limit which were stored in the attribute certificate. The count of available is stored in the database in a service provider, and judges whether it is contents use in the count limit recorded on the attribute certificate with reference to the management data in a database in a service provider.

[0297] The contents key which will be applied to decode of the contents stored in an attribute certification in the letter if judged with it being contents use in the count limit recorded on the attribute certificate: Perform decode of encryption data [of Kc]: [SP.Sto.K (Kc)]. A service provider performs decryption processing of encryption contents key: [SP.Sto.K (Kc)] stored in the attribute certificate using private key:SP.Sto.K which self owns, and takes out contents key:Kc.

[0298] Furthermore, a service provider updates the count management data of contents use in a database, and performs processing which carries out 1 decrement of the count of available to which the contents for use correspond. Furthermore, the contents key taken out in the service provider: Encipher by the session key (Kses) which generated Kc in previous mutual recognition processing, and transmit to the security chip of a user device.

[0299] (d5) If the contents key enciphered by the session key from the service provider, i.e., [Kses], (Kc) is received, the control section of a security chip will perform decryption processing using the session key held at the time of mutual recognition, and will acquire contents key:Kc. Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section.

[0300] (d6) Next, a user device control section acquires the encryption contents [Kc

(Content)] which should be decoded with the application of the acquired contents key from the memory in a security chip through the memory (for example, hard disk) or the security chip control section in a user device. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security (d7) chip is performed, the contents obtained as a decryption processing result are outputted to a user device control section, and a user (d8) device acquires contents. The contents key which acquired the control section of a security (d9) chip by decryption processing after these processings were completed: Cancel Kc and contents (Content).

[0301] Check processing of the count of contents use based on the attribute certificate (AC) by the service provider is performed by these processings. Only when it is in the restricted count of use, in a security chip, in the condition which can be decoded, it is re-enciphered and contents key:Kc is sent. Decode of contents with the contents key which the contents key was acquired in the security chip and acquired is performed, and contents use is attained in a user device.

[0302] In addition, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand.

[0303] (C) Off-line-buying-up contents, next the contents use conditions recorded on the attribute certificate are off-line processing, and explain processing from acquisition of the attribute certificate in the case of being buying-up contents to contents acquisition according to the sequence diagram of drawing 36 .

[0304] The processing sequence shown in drawing 36 has already shown the processing in the user device which is receipt ending about encryption contents, and is receipt ending about the attribute certificate which stored the use conditions corresponding to contents, and an encryption contents key from the service provider like drawing 34 explained previously and the processing sequence of drawing 35 , and shows processing of the security chip control section in a user device, a user device control section (high order software), and a service provider from the left.

[0305] The service provider ID acquisition processing from an attribute certificate in case, as for the maximum upper case (a), the attribute certificate is stored in the

internal memory of a security chip during the processing shown in drawing 36 , (b) shows the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in accessible memory at control of the external memory of a security chip, i.e., a user device control-section independent. These (a) and (b) are alternatively performed according to the storing location of an attribute certificate. Since each processing of (a) and (b) is the same as the processing in the case of the online time limitation explained with reference to drawing 34 , explanation is omitted. Acquisition of a service provider ID of either processing of (a) and (b) performs [next] the processing shown in drawing 36 (c), i.e., contents acquisition processing, by it.

[0306] (c1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the contents use demand which applied the attribute certificate to a security chip. The contents use conditions recorded on the attribute certificate in this example are off-line buying up.

[0307] (c2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. As for the control section of a security chip, in this verification processing, it is desirable to perform to verification of the public key certificate which followed on the high order, and performed a chain of verification, and the root certificate authority (CA) published from the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC). In addition, this chain verification may be indispensable.

[0308] (c3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, a security chip control section will take out encryption contents key: [SC.Stopub.SP.K (Kc)] stored in the attribute certificate, will perform decryption processing with the application of storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain, and will acquire contents key:Kc by it. Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section.

[0309] (c4) Next, a user device control section acquires the encryption contents [Kc

(Content)] which should be decoded with the application of the acquired contents key from the memory in a security chip through the memory (for example, hard disk) or the security chip control section in a user device. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security (c5) chip is performed, the contents obtained as a decryption processing result are outputted to a user device control section, and a user (c6) device acquires contents. The contents key which acquired the control section of a security (c7) chip by decryption processing after these processings were completed: Cancel Kc and contents (Content).

[0310] Decode of contents with the contents key which check processing of being the buying-up contents based on an attribute certificate (AC) was performed, contents key:Kc was decoded in the security chip by these processings, and the contents key was acquired, and was acquired is performed, and contents use is attained in a user device.

[0311] In addition, although considered as the configuration which applied the public key cryptosystem, used storage public key:SC.Stopub.SP.K corresponding to SP for encryption of a contents key, and used storage private key:SC.Stopri.SP.K corresponding to SP for decode of a contents key in the above-mentioned example of a configuration It is also possible to apply a common key system, and when applying a common key system, storage key (common key):SC.Sto.SP.K corresponding to SP is used for processing of the both sides of encryption of a contents key and a decryption. In this case, storage key (common key):SC.Sto.SP.K corresponding to SP is stored in the service provider management domain of a service provider where the memory of a security chip corresponds.

[0312] In addition, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand.

[0313] (D) The count limit contents of off-line-use, next the contents use conditions recorded on the attribute certificate are off-line processing, and explain processing from acquisition of the attribute certificate in the case of being the restricted contents which are a count of use to contents acquisition. When the use conditions of

an attribute certificate are the contents which have a count limit by off-line use, in order to perform count management within a user device based on the setups of an attribute certificate, it is necessary to have the management data of the count of contents use in a device. Possession processing of the management data of the count of contents use is import processing of the count management data of use.

[0314] (D-1) import **** -- explain import processing of the count management data of use first. There are a mode which manages the count of contents available with the security chip in a user device, and two modes which carry out storing management of the count management file at the external memory besides a security chip (for example, hard disk), and store only the hash value of management data in the memory in a security chip as management mode of the count of contents use.

[0315] With reference to drawing 37 , the import processing sequence of the count management data of use at the time of considering as the mode which manages the count of contents available with the security chip in a user device is explained first. Processing of the security chip control section in a user device, a user device control section (high order software), and a service provider is shown from the left. The security chip accompanying contents purchase processing and the mutual recognition between service providers are materialized, and the processing sequence of drawing 37 has already shown the processing after issue processing of the attribute certificate corresponding to the purchase contents to a security chip from the service provider. Here, it is recorded that the attribute certificates which a service provider publishes are the count limit contents of use in off-line use as contents use conditions, and the count of a contents use limit is recorded.

[0316] (1) If an attribute certificate is published and transmitted from a service provider, the control section of (2) security chip will perform verification processing of an attribute certificate. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. As for the control section of a security chip, in this verification processing, it is desirable to perform to verification of the public key certificate which followed on the high order, and performed a chain of verification, and the root certificate authority (CA) published from the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC). In addition, this chain verification may be indispensable.

[0317] (3) If the control section of a security chip judges with the contents use

conditions recorded on the attribute certificate being the count limit contents of off-line use, it will acquire each data of the application ID corresponding to a contents identifier, an attribute certificate (AC) serial number, and the count of a contents use limit from an attribute certificate. Furthermore, each data of user ID and a service provider ID inputted by the user at the time of purchase processing of contents is acquired through a user device control section, and such acquired applications ID, an attribute certificate (AC) serial number, and the count management data of contents use corresponding to each data of user ID verify whether it is registered to the service provider management domain of the memory in a security chip. In addition, since user ID etc. is held when the user logs in to a user device, a user device may transmit user ID and a service provider ID instead of a user inputting.

[0318] As mentioned above in the memory of a security chip, a service provider management domain will be set up for every registered service provider, and the count management data of contents use will be registered into the management domain. The example of a configuration of the count management data of contents use set as drawing 38 in the service provider management domain of the memory in a security chip is shown.

[0319] As shown in drawing 38 , AC serial (AC Serial#n) and the further remaining count data (Count#n) of available which are the application ID as a contents identifier (App.ID#n) and the identifier of a corresponding attribute certificate (AC) are matched and stored in a service provider management domain for every service provider ID and user ID. Even if it is the same contents, it has data composition which enabled the count count of use based on a different attribute certificate for every use user.

[0320] It returns to drawing 37 and explanation is continued about the sequence of import processing of the count management data of use. (3) The application ID corresponding to the contents identifier which acquired the control section of a security chip from the attribute certificate Each data of an attribute certificate (AC) serial number and the count of a contents use limit, The count management data of contents use corresponding to each data of user ID and a service provider ID inputted by the user If it checks that verify whether it is registered to the service provider management domain of the memory in a security chip, and the count management data of contents use is not registered into it (4) Additional registration of the count management data of contents use is carried out in a service provider management domain, an attribute certificate received message is generated after termination of (5) addition registration, and it transmits to a service provider.

[0321] In the example of drawing 37 , as for the attribute certificate (AC) received

from the service provider, each data of count:of application ID:0001 attribute (certificate AC) serial:1345 contents use limit 5 is recorded, and user input data is user ID:6737 service-provider ID:5678.

[0322] The control section of a security chip verifies whether the count management data of contents use corresponding to these data is in the service provider management domain where it corresponds in memory. In the data of SP management domain data (before updating) shown in drawing 37 , application ID:0001 and the data corresponding to attribute (certificate AC) serial:1345 do not exist as service provider ID:5678 and count management data of contents use corresponding to user ID:6737.

[0323] Therefore, processing which newly adds the count management data of contents use corresponding to the attribute certificate received from the service provider this time as service provider ID:5678 and count management data of contents use corresponding to user ID:6737 is performed. Consequently, the count of a contents use limit which application ID:0001 and the count management data of attribute (certificate AC) serial:1345 were added, and was recorded by the received attribute certificate as a count of available into the data of SP management-domain data (after updating) shown in the lower berth of drawing: 5 is set up.

[0324] Renewal of data which this count management data of contents use is referred to, carries out 1 decrement of the count of available to the utilization time of contents for every use, and is set to 5->4->3->2->1->0 is performed, the contents use after the count of available was set to 0 is refused, and contents use within the count of a use limit recorded on the attribute certificate is attained. About this contents use processing, it mentions later.

[0325] In addition, when the application ID of the attribute certificate received from the service provider and the same data as an attribute certificate (AC) serial are registered as count management data of contents use in the service provider ID which already corresponds, and the service provider management domain of user ID, it judges with it being issue of the duplicate attribute certificate, and additional registration of the count management data of contents use based on the attribute certificate is not performed.

[0326] Moreover, although it is the same as that of the application ID of the attribute certificate received from the service provider, when the data with which attribute certificate (AC) serials differ are registered as count management data of contents use in the service provider ID which already corresponds, and the service provider management domain of user ID, it judges with it being the attribute certificate which enables new use of the same contents based on a different attribute certificate, and

additional registration of the count management data of contents use based on the attribute certificate is performed.

[0327] That is, as count management data of contents use in the same service provider ID and the service provider management domain of the same user ID, even if it is the case where the data of application ID:0001 and count:of the AC serial:0001 remaining contents use 2 exist, it is already [0328]. Application ID: 0001AC serial: It remains 0002 and additional registration of the new management data of count:of contents use 5 is carried out.

[0329] The import processing flow of the count management data of use performed within the security chip at the time of considering as the mode which manages the count of contents available with the security chip in a user device to drawing 39 is shown. Each step is explained.

[0330] First, in step S221, Application ID, the count of a use limit, and an attribute certificate serial number are taken out from an attribute certificate (finishing [verification]). In step S222, it searches whether the count management data of the same application ID is having been stored in the attribute certificate in a service provider management domain [finishing / a setup in the memory in a security chip].

[0331] The count of a contents use limit recorded on the attribute certificate which progressed to step S225 and was received at step S223 according to the attribute certificate as application ID:nnnn, attribute (certificate AC) serial:mmmm, and a count of available when judged with there being no registration of the count management data of the same application ID: Set up x and perform count management data registration of use.

[0332] On the other hand, in step S223, when judged with the count management data of the same application ID being registered Progress to step S224 and it judges whether the count management data which is in agreement with the attribute certificate (AC) serial acquired from the attribute certificate further is registered to the service provider management domain in memory. When registered, it judges with it being duplication processing to the same attribute certificate, and new data registration is not performed but ends processing. When it judges with the count management data which is in agreement with the attribute certificate (AC) serial acquired from the attribute certificate on the other hand not being registered to the service provider management domain in memory The count of a contents use limit recorded on the attribute certificate which progressed to step S225 and was received according to the attribute certificate as application ID:nnnn, attribute (certificate AC) serial:mmmm, and count data of available: Set up x and register the count

management data of use.

[0333] Next, the import processing sequence of the count management data of use at the time of carrying out storing management of the count management file at the external memory besides a security chip (for example, hard disk), and considering as the processing mode which stores only the hash value of management data in the memory in a security chip with reference to drawing 40 , is explained. Processing of the security chip control section in a user device, a user device control section (high order software), and a service provider is shown from the left. The security chip accompanying contents purchase processing and the mutual recognition between service providers are materialized, and the processing sequence of drawing 40 has already shown the processing after issue processing of the attribute certificate corresponding to the purchase contents to a security chip from the service provider. Here, it is recorded that the attribute certificates which a service provider publishes are the count limit contents of use in off-line use as contents use conditions, and the count of a contents use limit is recorded.

[0334] It is the configuration of utilizing effectively the memory area where it was restricted in the security chip, and this processing mode carries out storing management of the real data file of count management data at the external memory besides a security chip (for example, hard disk), it is managing the hash (Hash) value of this external management file information inside a security chip, and makes it possible to verify the alteration of external management file information. A Hash Function is a function which considers a message as an input, compresses this into the data of predetermined bit length, and is outputted as a hash value. It is difficult for a Hash Function to predict an input from a hash value (output), and when 1 bit of the data inputted into the Hash Function changes, discovering different input data which many bits of a hash value change and has the same hash value has the difficult description. As a Hash Function, MD4, MD5, SHA-1, etc. may be used and DES-CBC may be used. In this case, MAC used as a final output value serves as a hash value.

[0335] The processing sequence shown in drawing 40 is explained. (1) If an attribute certificate is published and transmitted from a service provider, the control section of (2) security chip will perform verification processing of an attribute certificate. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. As for the control section of a security chip, in this verification processing, it is desirable to perform to

verification of the public key certificate which followed on the high order, and performed a chain of verification, and the root certificate authority (CA) published from the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC). In addition, this chain verification may be indispensable.

[0336] If the control section of a security chip judges with the contents use conditions recorded on the attribute certificate being the count limit contents of off-line use, it will perform read-out processing of the count management file from external memory. A count management file is in HDD which a user device control section manages by a diagram, and a count management file is read in (3) user device control section, and it is outputted to a security chip. Even if this read-out object is management file all data, it may be only data about the service provider corresponding to contents.

[0337] Next, the control section of a security chip develops the count management file which received from (4) user device control section to RAM in a security chip, and calculates a hash value based on expansion data. Count management data has the field configuration which stored two or more count management data matched with a service provider ID and user ID. The hash value is generated and stored in the service provider management domain in the memory of a security chip to the field data matched with a service provider ID and user ID.

[0338] It calculates a hash value by the control section of a security chip receiving from a user device control section, and extracting the field data corresponding to the service provider ID specified by the user and user ID from the count management file developed to RAM, and compares the calculated value with the hash value stored in the service provider management domain of the memory in a security chip. If a calculation hash value and a storing hash value are in agreement, it will judge with there being no alteration in data, and will progress to the next processing.

[0339] The corresponding field stored in the (service-provider SP) management domain where a hash value is computed based on service-provider ID:5678 of RAM expansion data, and the field data of user-ID:6737, and it corresponds in a security chip in the example of drawing, service-provider ID:5678 [i.e.,], user ID: It will compare with hash value:290a of 6737.

[0340] (5) Transmit the notice which shows the congruous purports when a hash value is in agreement to a user device control section, and when coincidence is not obtained, transmit an error message to a user device control section. (6) Next, the control section of a security chip acquires each data of the application ID

corresponding to a contents identifier, an attribute certificate (AC) serial number, and the count of a contents use limit from an attribute certificate. Furthermore, each data of user ID and a service provider ID inputted by the user at the time of purchase processing of contents is acquired through a user device control section, such acquired applications ID, an attribute certificate (AC) serial number, and the count management data of contents use corresponding to each data of user ID receive from a user device control section, and it verifies whether it is registered to the count management file developed to RAM.

[0341] If it checks that the count management data of contents use is not registered, the count management data of use of (7) contents is picked out from an attribute certificate (AC), additional registration is carried out at the count management file developed to RAM, the new hash value based on (8) additional data is calculated, and it stores in the corresponding field stored in the (service provider SP) management domain where it corresponds in (9) security chip. (10) After termination of additional registration, transmit to a user device with the count management file which updated the attribute certificate received message, and (11) user device stores the count management file which received in a hard disk.

[0342] In the example of drawing 40 , as for the attribute certificate (AC) received from the service provider, each data of count:of application ID:0001 attribute (certificate AC) serial:1345 contents use limit 5 is recorded, and user input data is user ID:6737 service-provider ID:5678.

[0343] The control section of a security chip verifies whether the count management data of contents use corresponding to these data is registered to the count management file developed to RAM. In the data in [RAM] SC of the maximum upper case shown in drawing 40 , application ID:0001 and the data corresponding to attribute (certificate AC) serial:1345 do not exist as service provider ID:5678 and count management data of contents use corresponding to user ID:6737.

[0344] Therefore, processing which newly adds the count management data of contents use corresponding to the attribute certificate received from the service provider this time as service provider ID:5678 and count management data of contents use corresponding to user ID:6737 is performed. Consequently, the count of a contents use limit which application ID:0001 and the count management data of attribute (certificate AC) serial:1345 were added, and was recorded by the received attribute certificate as a count of available into the data in [RAM] SC shown in the middle of drawing: 5 is set up.

[0345] Furthermore, service-provider ID:5678, user ID: A hash value is computed

based on the field data corresponding to 6737. In the example of drawing, the hash value before renewal of data is 290a, the hash value after renewal of data is 8731, and hash value:8731 of SP management domain of the bottom of drawing will be stored as an updating value.

[0346] While renewal of data which this count management data of contents use is referred to, carries out 1 decrement of the count of available to the utilization time of contents for every use, and is set to 5->4->3->2->1->0 is performed, a new hash value will be computed based on updating data, and an update process will be performed. About this contents use processing, it mentions later.

[0347] In addition, when the application ID of the attribute certificate received from the service provider and the same data as an attribute certificate (AC) serial are registered as the service providers ID and the count management data of contents use of the field of user ID with which the count management file which already received from the user device and was developed to RAM corresponds, it judges with it being issue of the duplicate attribute certificate, and additional registration of the count management data of contents use based on the attribute certificate is not performed.

[0348] Moreover, although it is the same as that of the application ID of the attribute certificate received from the service provider The data with which attribute certificate (AC) serials differ already receive from a user device. In being registered as the service provider ID and the count management data of contents use of the field of user ID with which the count management file developed to RAM corresponds It judges with it being the attribute certificate which enables new use of the same contents based on a different attribute certificate, and the additional registration of the count management data of contents use based on the attribute certificate and a hash value update process are performed.

[0349] Storing management of the count management file is carried out at the external memory besides a security chip (for example, hard disk), and the import processing flow of the count management data of use at the time of considering as the processing mode which stores only the hash value of management data in the memory in a security chip is shown in drawing 41 . Each step is explained.

[0350] First, in step S241, a count management file is read from external memory, the hash value based on the field data specified based on a service provider ID and user ID is computed in step S242, and it verifies whether it is in agreement with a calculation hash value and a hash value [finishing / storing in the service provider management domain in the memory of a security chip] (S243). When not in agreement,

it judges with the count management file read from external memory being altered, and error processing, for example, subsequent processing, is stopped.

[0351] A hash value is in agreement, when it judges with the count management file read from external memory not being altered, it progresses to step S244 and Application ID, the count of a use limit, and an attribute certificate serial number are taken out from an attribute certificate (finishing [verification]). Next, in step S245, it receives from a user device control section, and searches whether the count management data of the same application ID as what was stored in the attribute certificate is in the count management file developed to RAM.

[0352] The count of a contents use limit recorded on the attribute certificate which progressed to step S247 and was received at step S246 according to the attribute certificate as application ID:nnnn, attribute (certificate AC) serial:mmmm, and a count of available when judged with there being no registration of the count management data of the same application ID: Set up x and register the count management data of use.

[0353] On the other hand, in step S246, when judged with registration of the count management data of the same application ID being registered Progress to step S251 and it judges whether the count management data which is in agreement with the attribute certificate (AC) serial acquired from the attribute certificate further is registered to the count management file developed to RAM. When registered, it judges with it being duplication processing to the same attribute certificate, and new data registration is not performed but ends processing. When it judges with it not being registered to the count management file which the count management data which is in agreement with the attribute certificate (AC) serial acquired from the attribute certificate on the other hand developed to RAM The count of a contents use limit recorded on the attribute certificate which progressed to step S247 and was received according to the attribute certificate as application ID:nnnn, attribute (certificate AC) serial:mmmm, and a count of available: Set up x and perform count management data registration of use.

[0354] In step S247, if new count management data is written in the count management file developed to RAM according to an attribute certificate, in step S248, a new hash value is calculated based on data including new additional data, and a new hash value is stored in the corresponding field stored in the (service provider SP) management domain where it corresponds in a security chip. Furthermore, in step S249, renewal of the count management file stored in external memory (for example, hard disk) based on the updated count management file is performed.

[0355] Next, the contents use conditions recorded on the attribute certificate are off-line processing, and processing from acquisition of the attribute certificate in the case of being the count limit contents of use to contents acquisition is explained according to the sequence diagram of drawing 42 .

[0356] The processing sequence shown in drawing 42 has already shown the processing in the user device which is receipt ending about encryption contents, and is receipt ending about the attribute certificate which stored the use conditions corresponding to contents, and an encryption contents key from the service provider like drawing 34 explained previously, drawing 35 , and the processing sequence of drawing 36 , and shows processing of the security chip control section in a user device, a user device control section (high order software), and a service provider from the left.

[0357] The service provider ID acquisition processing from an attribute certificate in case, as for the maximum upper case (a), the attribute certificate is stored in the internal memory of a security chip during the processing shown in drawing 42 , (b) shows the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in accessible memory at control of the external memory of a security chip, i.e., a user device control-section independent. These (a) and (b) are alternatively performed according to the storing location of an attribute certificate. Since each processing of (a) and (b) is the same as the processing in the case of the online time limitation explained with reference to drawing 34 , explanation is omitted. Acquisition of a service provider ID of either processing of (a) and (b) performs [next] the processing shown in drawing 42 (c), i.e., contents acquisition processing, by it.

[0358] (c1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the contents use demand which applied the attribute certificate to a security chip. The contents use conditions recorded on the attribute certificate in this example are the count limits of off-line use.

[0359] (c2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. As for the control section of a security chip, in this verification processing, it

is desirable to perform to verification of the public key certificate which followed on the high order, and performed a chain of verification, and the root certificate authority (CA) published from the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC). In addition, this chain verification may be indispensable.

[0360] (c3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, by it, a security chip control section will perform an update process of count management data. About the detail of an update process of count management data, it mentions later. Furthermore, a security chip control section takes out encryption contents key: [SC.Stopub.SP.K (Kc)] stored in the attribute (c4) certificate, performs decryption processing with the application of storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain, and acquires contents key:Kc. Contents key: If it succeeds in acquisition of Kc, a security chip control section will notify that decode preparation of contents was completed to a user device control section.

[0361] (c5) Next, a user device control section acquires the encryption contents [Kc (Content)] which should be decoded with the application of the acquired contents key from the memory in a security chip through the memory (for example, hard disk) or the security chip control section in a user device. Furthermore, the acquired encryption contents are transmitted to a security chip, decryption processing which applied contents key:Kc to encryption contents within the security (c6) chip is performed, the contents obtained as a decryption processing result are outputted to a user device control section, and a user (c7) device acquires contents. The contents key which acquired the control section of a security (c8) chip by decryption processing after these processings were completed: Cancel Kc and contents (Content).

[0362] Decode of contents with the contents key which it restricted when it was contents use in the count limit of use of the contents based on an attribute certificate (AC), and contents key:Kc was decoded in the security chip by these processings, and the contents key was acquired, and was acquired is performed, and contents use is attained in a user device.

[0363] In addition, although considered as the configuration which applied the public key cryptosystem, used storage public key:SC.Stopub.SP.K corresponding to SP for encryption of a contents key, and used storage private key:SC.Stopri.SP.K corresponding to SP for decode of a contents key in the above-mentioned example of a configuration It is also possible to apply a common key system, and when applying a common key system, storage key (common key):SC.Sto.SP.K corresponding to SP is

used for processing of the both sides of encryption of a contents key and a decryption. In this case, storage key (common key):SC.Sto.SP.K corresponding to SP is stored in the service provider management domain of a service provider where the memory of a security chip corresponds.

[0364] In addition, as a distribution gestalt of the contents distribution to the user device from a service provider, or an attribute certificate (AC:Attribute Certificate), any gestalt of the gestalt performed based on the demand to the service provider from a user side and the gestalt (push type model) of the so-called push type which transmits to a target from a service provider on the other hand to the user who has made the subscriber contract regardless of the existence of a demand of a user is possible. In a push type model, a service provider will draw up and distribute the attribute certificate for target users (AC) beforehand.

[0365] Next, with reference to drawing 43 and drawing 44 , an update process of the count management data of use is explained. There are a mode which manages the count of contents available with the security chip in a user device as mentioned above, and two modes which carry out storing management of the count management file at the external memory besides a security chip (for example, hard disk), and store only the hash value of management data in the memory in a security chip as management mode of the count of contents available. It is drawing explaining the update process sequence of count management data [in / drawing 43 and / in drawing 44 / the latter mode]. [the former]

[0366] With reference to drawing 43 , the update process sequence of the count management data at the time of considering as the mode which manages a contents available time with the security chip in a user device is explained first. Processing of the security chip control section in a user device and a user device control section (high order software) is shown from the left. The processing sequence of drawing 43 shows subsequent processing as that to which verification of an attribute certificate can already be managed within the security chip.

[0367] (1) If the control section of a security chip judges with the contents use conditions recorded on the attribute certificate [finishing / verification] being the count limit contents of off-line use, it will acquire each data of the application ID corresponding to a contents identifier, an attribute certificate (AC) serial number, and the count of a contents use limit from an attribute certificate. Furthermore, each data of user ID and a service provider ID inputted by the user at the time of purchase processing of contents is acquired through a user device control section, and such acquired applications ID, an attribute certificate (AC) serial number, and the count

management data of contents use corresponding to each data of user ID verify whether it is registered to the service provider management domain of the memory in a security chip.

[0368] As mentioned above in the memory of a security chip, a service provider management domain will be set up for every registered service provider, and the count management data of contents use will be registered into the management domain.

[0369] In the example shown in drawing 43 , as for an attribute certificate (AC), each data of count:of application ID:0002 attribute (certificate AC) serial:3278 contents use limit 10 is recorded, and user input data is user ID:6737 service-provider ID:5678.

[0370] The control section of a security chip verifies whether the count management data of contents use corresponding to these data is in the service provider management domain where it corresponds in memory. in the data of SP management domain data (before updating) shown in drawing 43 , application ID:0002 and the data corresponding to attribute (certificate AC) serial:3278 exist as service provider ID:5678 and count management data of contents use corresponding to user ID:6737, and available -- it is set up with count (number of ** times):7.

[0371] (2) a security chip control section is available from this extract data -- perform decryption processing of (3) encryption contents key in which use of contents was stored by authorization, i.e., an attribute certificate, the condition [having checked that it is count (number of ** times):7>0, below the count of a limit further recorded on the attribute certificate, and that it was 10>=7, and these having been checked].

[0372] (4) A security chip control section performs further the data update process to which 1 **** of the counts of available of the associated data of the service provider management domain where it corresponds in memory is carried out. In this case, the count of available in application ID:0002 and the data corresponding to attribute (certificate AC) serial:3278 (the number of ** times): Perform processing which updates 7 to 6. In addition, decryption processing of the encryption contents key of (3) and an update process of the count management data of (4) may often also as a configuration which makes (3) behind for (4) previously perform procedure to juxtaposition.

[0373] Next, the update process sequence of the count management data at the time of carrying out storing management of the count management file at the external memory besides a security chip (for example, hard disk), and considering as the mode which stores only the hash value of management data in the memory in a security chip with reference to drawing 44 , is explained. Processing of the security chip control section in a user device and a user device control section (high order software) is

shown from the left. The processing sequence of drawing 44 shows subsequent processing as that to which verification of an attribute certificate can already be managed within the security chip.

[0374] If the control section of a security chip judges with the contents use conditions recorded on the attribute certificate being the count limit contents of off-line use, it will perform read-out processing of the count management file from external memory. A count management file is in HDD which a user device control section manages by a diagram, and a count management file is read in (1) user device control section, and it is outputted to a security chip. Even if this read-out object is management file all data, it may be only data about the service provider corresponding to contents.

[0375] Next, the control section of a security chip develops the count management file which received from (2) user device control section to RAM in a security chip, and calculates a hash value based on expansion data. Count management data has the field configuration which stored two or more count management data matched with a service provider ID and user ID. The hash value is generated and stored in the service provider management domain in the memory of a security chip to the field data matched with a service provider ID and user ID.

[0376] It calculates a hash value by the control section of a security chip receiving from a user device, and extracting the field data corresponding to the service provider ID specified by the user and user ID from the count management file developed to RAM, and compares the calculated value with the hash value stored in the service provider management domain of the memory in a security chip. If a calculation hash value and a storing hash value are in agreement, it will judge with there being no alteration in data, and will progress to the next processing.

[0377] The corresponding field stored in the (service-provider SP) management domain where a hash value is computed based on service-provider ID:5678 of RAM expansion data, and the field data of user-ID:6737, and it corresponds in a security chip in the example of drawing, service-provider ID:5678 [i.e.,], the hash value of user-ID:6737: It will compare with 8731.

[0378] (3) Transmit the notice which shows the congruous purports when a hash value is in agreement to a user device, and when coincidence is not obtained, transmit an error message to a user device. (4) Next, the control section of a security chip acquires each data of the application ID corresponding to a contents identifier, an attribute certificate (AC) serial number, and the count of a contents use limit from an attribute certificate. Furthermore, each data of user ID and a service provider ID

inputted by the user at the time of purchase processing of contents is acquired through a user device control section, such acquired applications ID, an attribute certificate (AC) serial number, and the count management data of contents use corresponding to each data of user ID receive from a user device, and it verifies whether it is registered to the count management file developed to RAM.

[0379] In the example shown in drawing 44 , as for an attribute certificate (AC), each data of count:of application ID:0002 attribute (certificate AC) serial:3278 contents use limit 10 is recorded, and user input data is user ID:6737 service-provider ID:5678.

[0380] The control section of a security chip verifies whether the count management data of contents use corresponding to these data is registered to the count management file developed to RAM. Into the data in [RAM] SC of the maximum upper case shown in drawing 44 , application ID:0002 and the data corresponding to attribute (certificate AC) serial:3278 exist as service provider ID:5678 and count management data of contents use corresponding to user ID:6737, and it is set up with :7 the number of available times (the number of ** times).

[0381] (5) a security chip control section is available from this extract data -- perform decryption processing of (6) encryption contents key in which use of contents was stored by authorization, i.e., an attribute certificate, the condition [having checked that it is count (number of ** times):7>0, below the count of a limit further recorded on the attribute certificate, and that it was 10>=7, and these having been checked].

[0382] (7) A security chip control section performs further the data update process to which 1 **** of the counts of available of the associated data of the count management file developed to RAM is carried out. In this case, the count of available in application ID:0002 and the data corresponding to attribute (certificate AC) serial:3278 (the number of ** times): Perform processing which updates 7 to 6.

[0383] Furthermore, a security chip control section calculates the new hash value based on the renewal data of (8), and stores it in the corresponding field stored in the (service provider SP) management domain where it corresponds in (9) security chip. The hash value of SP management domain of the bottom of drawing corresponding to [in the example of drawing 44 , the hash value based on application ID:0002 before updating and the field data corresponding to attribute (certificate AC) serial:3278 is 8731, and the hash value based on the data of this field after updating is set to bc35, and] service-provider ID:5678 and user-ID:6737: bc35 will be stored as an updating hash value.

[0384] (10) Transmit the updated count management file to a user device control section after termination of an update process, and a user device control section

stores the count management file which received in a hard disk.

[0385] Thus, while renewal of data which this count management data of contents use is referred to, carries out 1 decrement of the count of available to the utilization time of contents for every use, and is set to 5->4->3->2->1->0 is performed, a new hash value is computed based on updating data, an update process is performed, and contents use within the count of a use limit recorded on the attribute certificate is attained.

[0386] In the above, use of the contents according to the contents use conditions of an attribute certificate was explained. In addition, in the above-mentioned explanation, although time limitation and a count limit were explained separately After an attribute certificate with both limits of time limitation and a count limit is also possible and judging contents use propriety based on two conditions in these cases A contents key shall be decoded a condition [the check of being contents use in the term within the use condition set as the attribute certificate, and a count].

[0387] It explained that use of contents was performed in the user device which various use conditions, such as time limitation, a count limit, and buying up, are set to a [upgrade processing] attribute certificate as use conditions for contents, and has a security chip in it based on these use conditions. Next, the processing which changes a use limit of contents, such as modification of the count of a contents use limit set, for example as the attribute certificate or extension of time limitation, i.e., upgrade processing, is explained.

[0388] Specifically, there are various kinds of modes explained below in upgrade processing.

(1) Increase the count of available of the attribute certificate which recorded the count limit of use as contents use conditions. For example, he bought the ticket 10 times, and it remains 5 times, and increases to 10 times. He buys a ticket 10 times and usage OFF is increased for a ticket 10 times.

(2) Extend the use period of the attribute certificate which recorded use time limitation as contents use conditions. For example, a period is extended so that what can be used until after one week can be used until after one month. A period is extended so that the thing in which it became impossible to spend a period, having gone out can be used until after one month.

(3) Modification of the use conditions of the attribute certificate which recorded a count limit and time limitation as contents use conditions. For example, a count limit is changed into time limitation. Time limitation is changed into a count limit. A count limit is changed into buying up. Time limitation is changed into buying up.

(4) The album-ized contents data of an album-ized upgrade single string, For example, contents 1-n of plurality (n) stored in CD of one sheet, or DVD, Or there are a certain series-ized contents 1 - n, and it is purchase settled about these some. When the user holds the plurality of the attribute certificate 1 corresponding to purchased contents - the attribute certificate n in a user device, For example, when the attribute certificate 1 corresponding to contents 1, the attribute certificate 3 corresponding to contents 3, and the attribute certificate 5 corresponding to contents 5 are held to the user device, By showing a service provider these attribute certificates, the package (album) purchase of other contents which constitute an album, i.e., the contents of contents 2, 4, and 6 - n, can be carried out at a discount price.

[0389] There are various modes mentioned above in upgrade processing based on an attribute certificate. The outline of the activation sequence of this upgrade processing is as follows. First, a service provider (SP) shows a user device an upgrade menu, and a user chooses an upgrade menu. A user device transmits an upgrade demand command to a security chip according to assignment of a user with the tbe data of the attribute certificate [finishing / acquisition] made into an upgrade processing object. The control section of a security chip performs the communication link with a service provider, and transmits the attribute certificate [finishing / acquisition] made into an upgrade processing object to a service provider. After a service provider verifies the received attribute certificate, it performs upgrade processing which the user specified, publishes a new attribute certificate, and transmits to a security chip. In a user device, it becomes possible to use contents according to the use conditions of a new attribute certificate.

[0390] Upgrade processing in case the contents use conditions hereafter indicated by the attribute certificate (AC) used as the base of an upgrade are the following three modes is explained one by one.

(A) Count limit contents [of count limit (contents C) of online-use time limitation (contents B) online-use off-line-use0391] (A) upgrade **** which used the online-use time limitation attribute certificate (AC) as the base -- first, the contents use conditions recorded on the attribute certificate are on-line processing, and when it holds the attribute certificate with which use time limitation was set up, explain the upgrade processing which used this online-use time limitation attribute certificate as the base according to the sequence diagram of drawing 45 . Processing of the security chip control section in a user device, a user device control section (high order software), and a service provider is shown in drawing 45 from the left.

[0392] In drawing 45 , the service provider ID acquisition processing from an attribute

certificate in case the attribute certificate is stored in the internal memory of a security chip, and (b) the maximum upper case (a) The service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in accessible memory at control of the external memory of a security chip, i.e., a user device control-section independent, is shown. These (a) and (b) are alternatively performed according to the storing location of an attribute certificate. Mutual recognition processing of (c) and contents acquisition processing of (d) are performed in common.

[0393] First, it explains from processing of (a). (a1) A user device control section requires retrieval of the attribute certificate of an upgrade processing object of a security chip control section. (a2) A security chip control section outputs the list of attribute certificates [finishing / storing in the memory of a chip] to a user device control section, and displays a list by the attached browser in a user (a3) device. (a4) A user specifies the attribute certificate (AC) of an upgrade processing object from the displayed list, and transmits a read-out instruction to a security chip control section. (a5) A security chip control section reads the specified attribute certificate from an internal memory, outputs it to a user device control section, in a user (a6) device, displays an attribute certificate by the attached browser, and acquires the service provider identifier in attribute certificate storing data (SP ID).

[0394] It becomes processing of (b) when the attribute certificate is stored in accessible memory by control of the external memory of a security chip, i.e., a user device control-section independent. (b1) A user device control section performs a search of the attribute certificate of an upgrade processing object, in a user (b2) device, from AC list displayed by the attached browser, it specifies the attribute certificate (AC) of an upgrade processing object, is beginning to read it, displays an attribute certificate, and acquires the service provider identifier (SP ID) in attribute (b4) certificate storing data.

[0395] The service provider identifier (SP ID) acquired by either processing of the above (a) and (b) is used in order to acquire information required for mutual recognition from a service provider management domain. As mentioned above, the password input set up for every service provider is required for access to a service provider management domain, and by the password input corresponding to the service provider identifier (SP ID) acquired from the attribute certificate, a user performs access to a service provider management domain, and performs mutual recognition processing between the security chip shown in (c1) of drawing 45 , and a service provider.

[0396] This mutual recognition processing is performed as mutual recognition processing by TLS1.0 processing of drawing 16 explained previously, or other methods, for example, a public key system. In this mutual recognition processing, verification of a mutual public key certificate is made and the public key certificate to a root certificate authority (CA) is verified continuously if needed. In this authentication processing, a security chip and a service provider share a session key (Kses). Formation of mutual recognition performs [next] the processing shown in drawing 45 (d), i.e., upgrade attribute certification dictation profit processing.

[0397] (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the upgrade application demand of an attribute certificate, and upgrade conditions to a security chip. The upgrade conditions which the contents use conditions recorded on the attribute certificate of the upgrade processing object in this example are online time limitation, and a user specifies are modification (extension) of time limitation.

Time limitation -> to the count limit of online, it reversing-interval-restricts, -> buys up, and passes to the count limit of reversing interval limit -> off-line, and they are conditions, such as modification.

[0398] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) upgrade application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example.

[0399] Furthermore, it is desirable for the control section of a security chip to acquire the public key certificate linked according to the public key certificate information of AC holder in an attribute certificate (AC), and to verify a public key certificate if needed. For example, when the reliability of the publisher of an attribute certificate (AC) is uncertain, the judgment of whether to have the public key certificate of a certificate authority justly is attained by verifying the public key certificate of the publisher of an attribute certificate (AC). In addition, as the public key certificate mentioned above, when hierarchy organization is being made, it is desirable to perform to verification of the public key certificate which followed the path on the high order, and performed a chain of verification, and the root certificate authority (CA) published. In addition, this chain verification may be indispensable.

[0400] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip will send the attribute certificate of an upgrade processing object with the upgrade condition information specified by the user to a service provider. It is recorded on the attribute certificate of an upgrade processing object that they are online time limitation contents as use conditions, and expiration date data are stored in it. Furthermore, the data of the contents key enciphered by private key:SP.Sto.K which a service provider holds, i.e., [SP.Sto.K], (Kc) are stored.

[0401] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. If the justification of an attribute certificate is checked by these verification processings, upgrade attribute certificate generation processing based on the upgrade condition information specified by the user (d5) will be performed.

[0402] Upgrade attribute certificate generation processing is performed as processing which publishes an attribute certificate with a different serial number from the new attribute certificate which recorded the contents use conditions specified by the user, i.e., the attribute certificate received from the security chip. In addition, the historical data containing the serial of the attribute certificate used as the base of an upgrade are stored in the newly published upgrade attribute certification in the letter in this case.

[0403] In addition, the mode of an upgrade is modification (extension) of time limitation, as mentioned above.

Time limitation -> to the count limit of online, it reversing-interval-restricts, -> buys up and passes to the count limit of reversing interval limit -> off-line, and it is either of the modification and, in modification of time limitation, the upgrade attribute certificate which newly set up the use period is generated. Moreover, when changing into online or the count limit of off-line, the upgrade attribute certificate which stored the count of a use limit is generated. Moreover, it buys up, it passes, and when changing, the upgrade attribute certificate which considered contents use conditions as buying up is generated.

[0404] Although the contents key stored in an upgrade attribute certificate is stored like the original attribute certificate as a contents key [SP.Sto.K (Kc)] enciphered with the private key of a service provider when changing into modification of time limitation,

or the count limit of online To the count limit of off-line, buy up, pass, and modification or when changing the contents key which was enciphered in the upgrade attribute certificate with the public key corresponding to storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain of the security chip of a user device unlike the original attribute certificate -- that is [SC.Stopub.SP.K (Kc)] is stored.

[0405] In addition, it is the case where it considers as off-line processing, and when application of the common key system instead of a public key system is being performed, the contents key enciphered with the storage key (common key) corresponding to SP stored in the service provider management domain of the security chip of a user device is stored. In addition, when the service provider does not hold this common key, the storage key (common key) corresponding to SP is collectively sent at the time of sending of the attribute certificate from the security chip of the step (d3) of drawing 45 to a service provider. In this case, it enciphers and sends with the session key generated at the time of mutual recognition.

[0406] A service provider will send this to a security chip, if an upgrade attribute certificate is generated.

[0407] (d6) A security chip control section will perform verification processing of an attribute certificate, if the upgrade attribute certificate (AC) from a service provider is received. The check with the stored authority information (contents use conditions) in agreement with assignment conditions, a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable that the control section of a security chip performs chain verification of a public key certificate according to the public key certificate information of AC holder in an attribute certificate (AC) if needed. In addition, this chain verification may be indispensable.

[0408] (d7) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip transmits the upgrade attribute certificate confirmation of receipt to a service provider, and stores an upgrade (d8) attribute certificate in memory by it.

[0409] Furthermore, the control section of a security chip performs import processing of the count management data of use mentioned above by the utilization time of contents, when an upgrade attribute certificate is the count limit of off-line. The detail of import processing of the count management data of use is as having explained with reference to drawing 37 - drawing 41 previously, and has the mode which stores the

count of available in the interior of a security chip, and the mode which stores the count of available in external memory, and stores only a hash value in a security chip.
[0410] By the above processing, a user device acquires a new rise clade attribute certificate based on the already held attribute certificate, and the use of the contents according to the use conditions according to a rise clade attribute certificate of it is attained.
[0411] (B) The upgrade processing which used the count limit attribute certificate of online-use (AC) as the base, next the contents use conditions recorded on the attribute certificate are on-line processing, and when it holds the attribute certificate with which the count limit of use was set up, explain the upgrade processing which used this count limit attribute certificate of online-use as the base according to the sequence diagram of drawing 46 . Processing of the security chip control section in a user device, a user device control section (high order software), and a service provider is shown in drawing 46 from the left.
[0412] In drawing 46 , as for the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in the internal memory of a security chip, and (b), an attribute certificate shows the service provider ID acquisition processing from the attribute certificate in the case of being stored in the external memory of a security chip, i.e., memory accessible at user device control-section independent control, and (c of the maximum upper case (a)) is mutual recognition processing of a security chip and a service provider. These processings are the same as that of the case of above-mentioned drawing 45 , and omit explanation.
[0413] It explains from the processing after formation after mutual recognition. (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the upgrade application demand of an attribute certificate, and upgrade conditions to a security chip. The upgrade conditions which the contents use conditions recorded on the attribute certificate of the upgrade processing object in this example are the count limits of online, and a user specifies are modification (increment in a count) of the count of available.
Count limit of online -> to the count limit of the count limit -> off-line of modification online, it count[of modification online]-restricts, -> buys up, and passes to time limitation, and they are conditions, such as modification.
[0414] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) upgrade application demand from

a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable to perform the control section of a security chip if needed to verification of the public key certificate of AC holder in an attribute certificate (AC) and the public key certificate which verified the chain public key certificate and the root certificate authority (CA) published further. In addition, this chain verification may be indispensable.

[0415] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip will send the attribute certificate of an upgrade processing object with the upgrade condition information specified by the user to a service provider. It is recorded on the attribute certificate of an upgrade processing object that they are the count limit contents of online as use conditions, and the count of a use limit is stored in it. Furthermore, the data of the contents key enciphered by private key:SP.Sto.K which a service provider holds, i.e., [SP.Sto.K], (Kc) are stored.

[0416] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. If the justification of an attribute certificate is checked by these verification processings, upgrade attribute certificate generation processing based on the upgrade condition information specified by the user (d5) will be performed.

[0417] Upgrade attribute certificate generation processing is performed as processing which publishes an attribute certificate with a different serial number from the new attribute certificate which recorded the contents use conditions specified by the user, i.e., the attribute certificate received from the security chip. In addition, the historical data containing the serial of the attribute certificate used as the base of an upgrade are stored in the newly published upgrade attribute certification in the letter in this case.

[0418] In addition, the mode of an upgrade is modification (increment in a count) of the count of a use limit, as mentioned above.

Count limit of online -> to the count limit of the count limit -> off-line of modification online, it count[of modification online]-restricts, -> buys up, and passes to time

limitation, and it is either of the modification and, in modification of a count limit, the upgrade attribute certificate which newly set up the count of a use limit is generated. Moreover, when changing into time limitation, the upgrade attribute certificate which stored time limitation information is generated.

[0419] When changing the count of a use limit as a count limit of online and changing into time limitation Although the contents key stored in an upgrade attribute certificate is stored like the original attribute certificate as a contents key [SP.Sto.K (Kc)] enciphered with the private key of a service provider To the count limit of off-line, buy up, pass, and modification or when changing the contents key which was enciphered in the upgrade attribute certificate with the public key corresponding to storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain of the security chip of a user device unlike the original attribute certificate -- that is [SC.Stopub.SP.K (Kc)] is stored.

[0420] In addition, it is the case where it considers as off-line processing, and when application of the common key system instead of a public key system is being performed, the contents key enciphered with the storage key (common key) corresponding to SP stored in the service provider management domain of the security chip of a user device is stored. In addition, when the service provider does not hold this common key, the storage key (common key) corresponding to SP is collectively sent at the time of sending of the attribute certificate from the security chip of the step (d3) of drawing 46 to a service provider. In this case, it enciphers and sends with the session key generated at the time of mutual recognition.

[0421] A service provider will send this to a security chip, if an upgrade attribute certificate is generated.

[0422] (d6) A security chip control section will perform verification processing of an attribute certificate, if the upgrade attribute certificate (AC) from a service provider is received. The check with the stored authority information (contents use conditions) in agreement with assignment conditions, a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable that the control section of a security chip performs chain verification of a public key certificate according to the public key certificate information of AC holder in an attribute certificate (AC) if needed. In addition, this chain verification may be indispensable.

[0423] (d7) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip

transmits the upgrade attribute certificate confirmation of receipt to a service provider, and stores an upgrade (d8) attribute certificate in memory by it.

[0424] Furthermore, the control section of a security chip performs import processing of the count management data of use mentioned above by the utilization time of contents, when an upgrade attribute certificate is the count limit of off-line. The detail of the count management data import processing of use is as having explained with reference to drawing 37 - drawing 41 previously, and has the mode which stores the count of available in the interior of a security chip, and the mode which stores the count of available in external memory, and stores only a hash value in a security chip.

[0425] By the above processing, a user device acquires a new rise clade attribute certificate based on the already held attribute certificate, and the use of the contents according to the use conditions according to a rise clade attribute certificate of it is attained.

[0426] (C) The upgrade processing which used the count limit attribute certificate of off-line-use (AC) as the base, next the contents use conditions recorded on the attribute certificate are off-line processing, and when it holds the attribute certificate with which the count limit of use was set up, explain the upgrade processing which used this count limit attribute certificate of off-line-use as the base according to the sequence diagram of drawing 47 . Processing of the security chip control section in a user device, a user device control section (high order software), and a service provider is shown in drawing 47 from the left.

[0427] In drawing 47 , as for the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in the internal memory of a security chip, and (b), an attribute certificate shows the service provider ID acquisition processing from the attribute certificate in the case of being stored in the external memory of a security chip, i.e., memory accessible at user device control-section independent control, and (c of the maximum upper case (a)) is mutual recognition processing of a security chip and a service provider. These processings are the same as that of the case of above-mentioned drawing 45 , and omit explanation.

[0428] It explains from the processing after formation after mutual recognition. (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the upgrade application demand of an attribute certificate, and upgrade conditions to a security chip. The upgrade conditions which the contents use conditions recorded on the attribute certificate of the upgrade processing object in this example are the

count limits of off-line, and a user specifies are modification (increment in a count) of the count of available.
Count limit of off-line -> to the count limit of the count limit -> online of modification off-line, it count[of modification off-line]-restricts, -> buys up, and passes to time limitation, and they are conditions, such as modification.
[0429] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) upgrade application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable to perform the control section of a security chip if needed to verification of the public key certificate of AC holder in an attribute certificate (AC) and the public key certificate which verified the chain public key certificate and the root certificate authority (CA) published further. In addition, this chain verification may be indispensable.
[0430] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip will send the attribute certificate of an upgrade processing object with the upgrade condition information specified by the user to a service provider. It is recorded on the attribute certificate of an upgrade processing object that they are the count limit contents of off-line as use conditions, and the count of a use limit is stored in it. Furthermore, the contents key enciphered with the public key corresponding to storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain of the security chip of a user device, i.e., [SC.Stopub.SP.K], (Kc) is stored.
[0431] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. If the justification of an attribute certificate is checked by these verification processings, upgrade attribute certificate generation processing based on the upgrade condition information specified by the user (d5) will be performed.
[0432] Upgrade attribute certificate generation processing is performed as processing which publishes an attribute certificate with a different serial number from the new

attribute certificate which recorded the contents use conditions specified by the user, i.e., the attribute certificate received from the security chip. In addition, the historical data containing the serial of the attribute certificate used as the base of an upgrade are stored in the newly published upgrade attribute certification in the letter in this case.

[0433] In addition, the mode of an upgrade is modification (increment in a count) of the count of a use limit, as mentioned above.

Count limit of off-line -> to the count limit of the count limit -> online of modification off-line, it count[of modification off-line]-restricts, -> buys up, and passes to time limitation, and it is either of the modification and, in modification of a count limit, the upgrade attribute certificate which newly set up the count of a use limit is generated. Moreover, when changing into time limitation, the upgrade attribute certificate which stored time limitation information is generated.

[0434] Buy up, when changing the count of a use limit as a count limit of off-line, and when passing and changing The contents key stored in an upgrade attribute certificate Although stored as the contents key enciphered with the public key corresponding to storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain as well as the original attribute certificate, i.e., [SC.Stopub.SP.K], (Kc) When you change into time limitation to modification or the count limit of online, unlike the original attribute certificate, let the contents key stored in an upgrade attribute certificate be the contents key [SP.Sto.K (Kc)] enciphered with the private key of a service provider.

[0435] In addition, it is the case where it considers as off-line processing, and when application of the common key system instead of a public key system is being performed, the contents key enciphered with the storage key (common key) corresponding to SP stored in the service provider management domain of the security chip of a user device is stored. In addition, when the service provider does not hold this common key, the storage key (common key) corresponding to SP is collectively sent at the time of sending of the attribute certificate from the security chip of the step (d3) of drawing 47 to a service provider. In this case, it enciphers and sends with the session key generated at the time of mutual recognition.

[0436] A service provider will send this to a security chip, if an upgrade attribute certificate is generated.

[0437] (d6) A security chip control section will perform verification processing of an attribute certificate, if the upgrade attribute certificate (AC) from a service provider is received. The check with the stored authority information (contents use conditions) in

agreement with assignment conditions, a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable that the control section of a security chip performs chain verification of a public key certificate according to the public key certificate information of AC holder in an attribute certificate (AC) if needed. In addition, this chain verification may be indispensable.

[0438] (d7) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip transmits the upgrade attribute certificate confirmation of receipt to a service provider, and stores an upgrade (d8) attribute certificate in memory by it.

[0439] Furthermore, the control section of a security chip performs import processing of the count management data of use mentioned above by the utilization time of contents, when an upgrade attribute certificate is the count limit of off-line. The detail of the count management data import processing of use is as having explained with reference to drawing 37 - drawing 41 previously, and has the mode which stores the count of available in the interior of a security chip, and the mode which stores the count of available in external memory, and stores only a hash value in a security chip.

[0440] By the above processing, a user device acquires a new rise clade attribute certificate based on the already held attribute certificate, and the use of the contents according to the use conditions according to a rise clade attribute certificate of it is attained.

[0441] (D) An album purchase mold upgrade, next a series of album-ized contents data, For example, contents 1-n of plurality (n) stored in CD of one sheet, or DVD, Or there are a certain series-ized contents 1 - n, and it is purchase settled about these some. When the user holds the plurality of the attribute certificate 1 corresponding to purchased contents - the attribute certificate n in a user device, by showing a service provider these attribute certificates The upgrade processing considered as the processing which carries out package (album) purchase of other contents which constitute an album, i.e., the contents of contents 2, 4, and 6 - n, at a discount price is explained with reference to drawing 48 .

[0442] Drawing 48 shows processing of the security chip control section in a user device, a user device control section (high order software), and a service provider from the left. As for the service provider ID acquisition processing from an attribute certificate in case the attribute certificate is stored in the internal memory of a security chip, and (b), an attribute certificate shows the service provider ID

acquisition processing from the attribute certificate in the case of being stored in the external memory of a security chip, i.e., memory accessible at user device control-section independent control, and (c of the maximum upper case (a)) is mutual recognition processing of a security chip and a service provider. These processings are the same as that of the case of above-mentioned drawing 45 , and omit explanation.

[0443] It explains from the processing after formation after mutual recognition. (d1) A user checks the authority information on the attribute certificate displayed by the browser of attachment of a user device (contents use conditions), and outputs the upgrade application demand of an attribute certificate, and upgrade conditions to a security chip. The attribute certificates of the upgrade processing object in this example are one or more attribute certificates corresponding to some contents which constitute the album identified as a set pair of two or more of a certain contents. other parts from which the upgrade conditions which a user specifies constitute an album -- they are conditions, such as the purchase of all other contents that constitute the purchase album of contents.

[0444] (d2) A security chip control section will perform verification processing of an attribute certificate, if the attribute (certificate AC) upgrade application demand from a user device control section is received. The check of authority information (contents use conditions), a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable to perform the control section of a security chip if needed to verification of the public key certificate of AC holder in an attribute certificate (AC) and the public key certificate which verified the chain public key certificate and the root certificate authority (CA) published further. In addition, this chain verification may be indispensable.

[0445] (d3) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip will send the attribute certificate of an upgrade processing object with the upgrade condition information specified by the user to a service provider.

[0446] (d4) The service provider which received the attribute certificate from the security chip performs signature verification processing of an attribute certificate. Moreover, it is desirable in this case to verify continuously the public key certificate linked to an attribute certificate and its high order public key certificate. In addition, this chain verification may be indispensable. If the justification of an attribute

certificate is checked by these verification processings, upgrade attribute certificate generation processing based on the upgrade condition information specified by the user (d5) will be performed.

[0447] Upgrade attribute certificate generation processing is performed as processing which publishes an attribute certificate with a different serial number from the new attribute certificate which recorded the contents use conditions specified by the user, i.e., the attribute certificate received from the security chip. In addition, the historical data containing the serial of the attribute certificate used as the base of an upgrade are stored in the newly published upgrade attribute certification in the letter in this case.

[0448] in addition, other parts which the others which constitute an album are either of the purchase of all other contents that constitute the purchase album of contents a part, and constitute an album as the mode of an upgrade was mentioned above -- the case of the purchase of contents -- a part of purchase assignment -- the upgrade attribute certificate corresponding to contents is generated. Moreover, in the purchase of all other contents that constitute an album, the upgrade attribute certificate corresponding to all other contents that constitute an album is generated.

[0449] In addition, the use conditions in this case are possible also for a user specifying beforehand, and good also as a configuration for which a service provider opts. When a user specifies, it specifies in the step (d1) of drawing 48 , and assignment conditions are collectively sent at the time of sending of the attribute certificate from the security chip of (d3) to a service provider.

[0450] When generating the upgrade attribute certificate considered as off-line use, a service provider The contents key [SC.Stopub.SP.K (Kc)] enciphered with the public key corresponding to storage private key:SC.Stopri.SP.K corresponding to SP stored in the service provider management domain is stored. When you generate the upgrade attribute certificate considered as online use, let the contents key stored in an upgrade attribute certificate be the contents key [SP.Sto.K (Kc)] enciphered with the private key of a service provider.

[0451] In addition, it is the case where it considers as off-line processing, and when application of the common key system instead of a public key system is being performed, the contents key enciphered with the storage key (common key) corresponding to SP stored in the service provider management domain of the security chip of a user device is stored. In addition, when the service provider does not hold this common key, the storage key (common key) corresponding to SP is collectively sent at the time of sending of the attribute certificate from the security

chip of the step (d3) of drawing 48 to a service provider. In this case, it enciphers and sends with the session key generated at the time of mutual recognition.
[0452] A service provider will send this to a security chip, if an upgrade attribute certificate is generated.
[0453] (d6) A security chip control section will perform verification processing of an attribute certificate, if the upgrade attribute certificate (AC) from a service provider is received. The check with the stored authority information (contents use conditions) in agreement with assignment conditions, a format check, and signature verification processing are included in verification processing. Signature verification processing is performed according to the same sequence as the processing flow of drawing 20 explained previously, for example. Furthermore, it is desirable that the control section of a security chip performs chain verification of a public key certificate according to the public key certificate information of AC holder in an attribute certificate (AC) if needed. In addition, this chain verification may be indispensable.
[0454] (d7) If the judgment without the alteration of an attribute certificate is obtained by verification of an attribute certificate, the control section of a security chip transmits the upgrade attribute certificate confirmation of receipt to a service provider, and stores an upgrade (d8) attribute certificate in memory by it.
[0455] Furthermore, the control section of a security chip performs import processing of the count management data of use mentioned above by the utilization time of contents, when an upgrade attribute certificate is the count limit of off-line. The detail of the count management data import processing of use is as having explained with reference to drawing 37 - drawing 41 previously, and has the mode which stores the count of available in the interior of a security chip, and the mode which stores the count of available in external memory, and stores only a hash value in a security chip.
[0456] By the above processing, a user device acquires a new rise clade attribute certificate based on the already held attribute certificate, and the use of the contents according to the use conditions according to a rise clade attribute certificate of it is attained.
[0457] As for the right information stored in the storage means in the user device with which a [data backup and restoration-processing] user purchases from a service provider, and has a security chip, and a certification document, it is desirable to back up in preparation for the situation of disappearance. There are information which may be seen, and information which must be held to secure one as information which should back up. The information which may be seen is certification documents, such as a public key certificate and an attribute certificate. With the information held to

secure one, there is information of evidence on the service subscription currently written in the service provider management domain of for example, a security chip etc.
[0458] About certification documents, such as a public key certificate and an attribute certificate, it is enough that a user stores duplicate information in the memory card which carried the hard disk and the flash memory suitably. Although the contents key is stored in the attribute certificate, since connection with a service provider is needed in online use and the justification of a device (security chip) is checked at the time of the mutual recognition in this case, contents are not used unjustly. Moreover, since the key for decoding a contents key also in the case of off-line use is stored in the service provider management domain of security CHIBBU, it becomes able [only an authorized user] for access with the password which held and mentioned above the security chip of a valid-user device to decode an encryption contents key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing explaining the outline of the contents use managerial system configuration of this invention.
[Drawing 2] It is drawing showing a format of an applicable public key certificate in the contents use managerial system of this invention.
[Drawing 3] It is drawing showing a format of an applicable public key certificate in the contents use managerial system of this invention.
[Drawing 4] It is drawing showing a format of an applicable public key certificate in the contents use managerial system of this invention.

[Drawing 5] It is drawing showing a format of the attribute certificate as an applicable authority information certificate in the contents use managerial system of this invention.
[Drawing 6] It is the block diagram showing the configuration of the security chip in a user device.
[Drawing 7] It is drawing showing the main data used as the processing object within a user device.
[Drawing 8] It is drawing showing the initial registration processing sequence of authentication information (password).
[Drawing 9] It is drawing showing the modification processing sequence of authentication information (password).
[Drawing 10] It is drawing showing the modification processing sequence of authentication information (password).
[Drawing 11] It is drawing explaining correspondence with authentication information (password) and a master password.
[Drawing 12] It is drawing explaining distribution processing of a master password.
[Drawing 13] It is drawing showing the recurrence line processing sequence of a master password.
[Drawing 14] It is the flow Fig. showing calculation processing of a master password.
[Drawing 15] It is drawing showing attribute certificate (AC) issue and a contents reception sequence.
[Drawing 16] It is drawing showing the sequence of the TLS1.0 handshake protocol which is the example of mutual recognition processing.
[Drawing 17] It is drawing explaining generation processing of MAC applied to data alteration verification.
[Drawing 18] It is drawing showing the issue processing sequence of an attribute certificate (AC).
[Drawing 19] It is a flow Fig. explaining the ECDSA signature generation procedure which is the example of signature generation processing.
[Drawing 20] It is a flow Fig. explaining the ECDSA signature verification procedure which is the example of signature verification processing.
[Drawing 21] It is drawing explaining correlation with a public key certificate (PKC) and an attribute certificate (AC).
[Drawing 22] It is drawing showing the verification processing flow of a public key certificate (PKC).
[Drawing 23] It is drawing showing the verification processing flow (Example 1) of an

attribute certificate (AC).

[Drawing 24] It is drawing showing the verification processing flow (Example 2) of an attribute certificate (AC).

[Drawing 25] It is a sequence diagram explaining contents use processing (off-line) in which the attribute certificate (AC) was used.

[Drawing 26] It is a sequence diagram explaining contents use processing (online) in which the attribute certificate (AC) was used.

[Drawing 27] It is drawing explaining contents use processing (off-line) in which the attribute certificate (AC) which stored the encryption data of a contents key with a global common key was used.

[Drawing 28] It is a sequence diagram explaining an update process of a global common key.

[Drawing 29] It is a sequence diagram explaining an update process of a global common key.

[Drawing 30] It is drawing explaining the decryption processing using a decoder.

[Drawing 31] It is drawing explaining the decryption processing sequence using a decoder.

[Drawing 32] It is drawing explaining the decryption processing flow using a decoder.

[Drawing 33] It is a flow Fig. explaining application processing of the attribute certificate by the side of a user device (AC).

[Drawing 34] It is a sequence diagram explaining use processing of the online time limitation contents using an attribute certificate (AC).

[Drawing 35] It is a sequence diagram explaining use processing of the count limit contents of online using an attribute certificate (AC).

[Drawing 36] It is a sequence diagram explaining use processing of the off-line buying-up contents using an attribute certificate (AC).

[Drawing 37] It is drawing explaining import processing of the count management data of use corresponding to the count limit contents of off-line.

[Drawing 38] It is drawing showing the example of a data configuration of the count management data of use corresponding to the count limit contents of off-line.

[Drawing 39] It is a flow Fig. explaining import processing of the count management data of use corresponding to the count limit contents of off-line.

[Drawing 40] It is drawing explaining import processing of the count management data of use of the hash value management mold corresponding to the count limit contents of off-line.

[Drawing 41] It is a flow Fig. explaining import processing of the count management

data of use of the hash value management mold corresponding to the count limit contents of off-line.

[Drawing 42] It is drawing explaining the contents use processing which applied the attribute certificate of the count limit contents of off-line.

[Drawing 43] It is drawing explaining an update process of the count management data corresponding to the count limit contents of off-line.

[Drawing 44] It is drawing explaining an update process of the count management data of the hash value management mold corresponding to the count limit contents of off-line.

[Drawing 45] It is drawing explaining the upgrade processing which applied the online time limitation attribute certificate as the base.

[Drawing 46] It is drawing explaining the upgrade processing which applied the count limit attribute certificate of online as the base.

[Drawing 47] It is drawing explaining the upgrade processing which applied the count limit attribute certificate of off-line as the base.

[Drawing 48] It is drawing explaining upgrade processing of an album purchase mold.

[Drawing 49] It is drawing explaining the outline of data restoration processing by the support center.

[Drawing 50] It is drawing explaining the processing sequence outline of data restoration processing by the support center.

[Drawing 51] It is drawing explaining the data backup processing sequence performed by the user device side.

[Drawing 52] It is drawing explaining the outline of the backup data read-out processing by the support center.

[Drawing 53] It is drawing explaining the data restoration-processing sequence by the support center.

[Drawing 54] It is drawing showing the example of a configuration of a user device.

[Drawing 55] It is drawing showing the example of a configuration of each entity, such as a service provider, a support center, and a contents creator.

[Description of Notations]

101 User Device

102 Service Provider

103 Contents Creator

104 User Device Manufacturer

105 Support Center

106 Certificate Authority

110 Attribute Certificate

200 User Device
201 CPU (Central processing Unit)
202 Interface
203 ROM(Read-Only-Memory)
204 RAM(Random Access Memory)
205 Cipher-Processing Section
206 Memory Section
210 Security Chip
221 User Device Side Control Section
222 External Memory Section
280 Decoder
301 System Holder
302 Service Provider
303 Contents Creator
304 User Device
410 User Device
411 Security Chip
421 Storage Means
422 Storage Media
430 User Device
450 Support Center
470 User Device
471 Storage Media
472 User Device
475 Support Center
501 CPU (Central processing Unit)
502 ROM(Read-Only-Memory)
503 RAM(Random Access Memory)
504 HDD
505 Input Section
506 Output Section
507 Communications Department
508 Drive
509 Removable Record Medium
510 Bus
511 Input/output Interface

512 Security Chip

601 CPU(Central processing Unit)

602 ROM(Read-Only-Memory)

603 RAM(Random Access Memory)

604 HDD

605 Cipher-Processing Means

606 Drive

607 Removable Record Medium

608,609 Communications department

610 Bus

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－85321
（P2003－85321A）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１４２	Ｇ０６Ｆ　17/60	１４２	５Ｃ０６４
	３０２		３０２Ｅ	５Ｊ１０４
	５１２		５１２	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｎ　7/167			６０１Ｅ	

審査請求　未請求　請求項の数30　ＯＬ　（全 91 頁）　最終頁に続く

(21)出願番号　特願2001－274854(P2001－274854)

(22)出願日　平成13年９月11日(2001.9.11)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

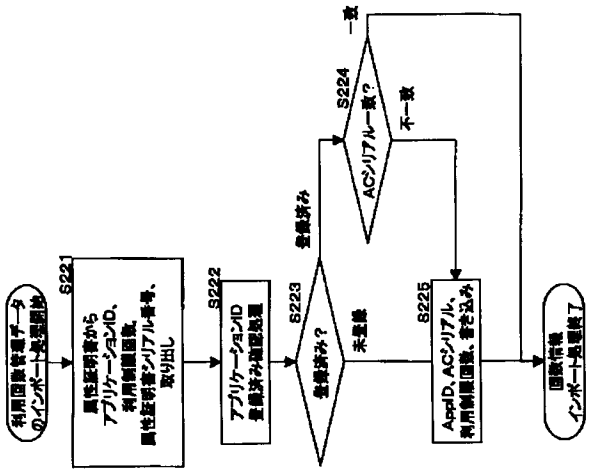
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラム

(57)【要約】
【課題】　サービスプロバイダ側でのユーザのコンテンツ利用権限管理を不要とし、コンテンツ利用条件のアップグレードを可能としたシステムを実現する。
【解決手段】　暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容するシステムにおいて、サービスプロバイダが、ユーザからコンテンツ利用権限証明書を受信し、コンテンツ利用権限証明書の発行エンティティの電子署名の検証によりデータ改竄のないことの確認を条件として、ユーザ情報およびユーザのコンテンツ購入情報をコンテンツ利用権限証明書から取得し、利用条件変更等のアップグレード処理を行なう。ユーザ管理データを、サービスプロバイダ側で保有することなく、コンテンツ利用条件変更処理等が可能となる。



1

【特許請求の範囲】

【請求項１】コンテンツの利用を行なうユーザデバイスと、

コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有し、

前記ユーザデバイスは、

前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用を行なう構成を有するとともに、

前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報の変更処理要求を実行する構成を有し、

前記サービスプロバイダは、

前記ユーザデバイスからのコンテンツ利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とするコンテンツ利用権限管理システム。

【請求項２】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、

前記ユーザデバイスは、

前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であることの判定を条件として、前記暗号化コンテンツ鍵の復号を実行してコンテンツ鍵を取得する構成であることを特徴とする請求項１に記載のコンテンツ利用権限管理システム。

【請求項３】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、

前記ユーザデバイスは、

コンテンツ利用に際して、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、ユーザデバイス内に格納した鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ利用権限管理システム。

【請求項４】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、

前記サービスプロバイダは、

2

ユーザデバイスにおけるコンテンツ利用に際して、該ユーザデバイスから送付済みコンテンツ利用権限証明書を受信し、受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、サービスプロバイダ固有鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ利用権限管理システム。

【請求項５】前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報は、コンテンツ利用期間制限情報、コンテンツ利用回数制限情報、利用制限を設けないコンテンツ買い切りの３態様のいずれかであり、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求は、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを含み、

前記サービスプロバイダは、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ利用権限管理システム。

【請求項６】前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、

サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、

前記サービスプロバイダは、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ利用権限管理システム。

【請求項７】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティテイの電子署名が

付加された構成であり、
前記サービスプロバイダは、
前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする請求項１に記載のコンテンツ利用権限管理システム。
【請求項８】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、
前記サービスプロバイダは、
前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする請求項１に記載のコンテンツ利用権限管理システム。
【請求項９】前記コンテンツ利用権限証明書は、属性証明書認証局の発行する属性証明書であり、
コンテンツの復号に適用するコンテンツ鍵を暗号化した暗号化コンテンツ鍵を、属性証明書中の属性情報フィールドに格納した構成であることを特徴とする請求項１に記載のコンテンツ利用権限管理システム。
【請求項１０】前記コンテンツ利用権限証明書は、属性証明書認証局の発行する属性証明書であり、
属性証明書中の属性情報フィールドに、コンテンツの利用条件を格納した構成であることを特徴とする請求項１に記載のコンテンツ利用権限管理システム。
【請求項１１】コンテンツの利用を行なうユーザデバイスと、
購入コンテンツ情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有し、
前記ユーザデバイスは、
前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、
前記サービスプロバイダは、
前記ユーザデバイスから受信したコンテンツ利用権限証明書に格納されたコンテンツ情報に基づいて、該コンテンツ情報と同一の集合コンテンツとして識別される同一アルバムに属するコンテンツに対応するコンテンツ利用権限証明書をアップグレードコンテンツ利用権限証明書として生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とするコンテンツ利用権限管理システム。
【請求項１２】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、
前記サービスプロバイダは、
前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする請求項１１に記載のコンテンツ利用権限管理システム。
【請求項１３】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、
前記サービスプロバイダは、
前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする請求項１１に記載のコンテンツ利用権限管理システム。
【請求項１４】コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおけるコンテンツ利用権限管理方法であり、
前記ユーザデバイスは、
前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報の変更処理要求を実行し、
前記サービスプロバイダは、
前記ユーザデバイスからのコンテンツ利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とするコンテンツ利用権限管理方法。
【請求項１５】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、
前記ユーザデバイスは、
前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であることの判定を条件として、前記暗号化コンテンツ鍵の復号を実行してコンテンツ鍵を取得することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。
【請求項１６】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、
前記ユーザデバイスは、
コンテンツ利用に際して、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得ら

れたことを条件として、ユーザデバイス内に格納した鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項１７】前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、

前記サービスプロバイダは、

ユーザデバイスにおけるコンテンツ利用に際して、該ユーザデバイスから送付済みコンテンツ利用権限証明書を受信し、受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、サービスプロバイダ固有鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項１８】前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報は、コンテンツ利用期間制限情報、コンテンツ利用回数制限情報、利用制限を設けないコンテンツ買い切りの３態様のいずれかであり、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求は、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを含み、

前記サービスプロバイダは、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項１９】前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、

サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、

前記サービスプロバイダは、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項２０】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、

前記サービスプロバイダは、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項２１】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記サービスプロバイダは、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行することを特徴とする請求項１４に記載のコンテンツ利用権限管理方法。

【請求項２２】コンテンツの利用を行なうユーザデバイスと、購入コンテンツ情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおけるコンテンツ利用権限管理方法であり、

前記ユーザデバイスは、

前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、

前記サービスプロバイダは、

前記ユーザデバイスから受信したコンテンツ利用権限証明書に格納されたコンテンツ情報に基づいて、該コンテンツ情報と同一の集合コンテンツとして識別される同一アルバムに属するコンテンツに対応するコンテンツ利用権限証明書をアップグレードコンテンツ利用権限証明書として生成し、ユーザデバイスに対して送信する処理を実行することを特徴とするコンテンツ利用権限管理方法。

【請求項２３】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、

前記サービスプロバイダは、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件

として実行することを特徴とする請求項２２に記載のコンテンツ利用権限管理方法。

【請求項２４】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記サービスプロバイダは、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行することを特徴とする請求項２２に記載のコンテンツ利用権限管理方法。

【請求項２５】コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおいて、コンテンツ利用権限証明書を発行する情報処理装置であり、

ユーザデバイスから発行済みのコンテンツ利用条件情報を伴うコンテンツ利用条件変更処理要求を受信し、

受信したコンテンツ利用権限証明書の検証処理を実行し、

該検証により前記コンテンツ利用権限証明書の正当性が確認されたことを条件として、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする情報処理装置。

【請求項２６】前記情報処理装置は、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする請求項２５に記載の情報処理装置。

【請求項２７】前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、

サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、

前記情報処理装置は、

前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする請求項２５に記載の情報処理装置。

【請求項２８】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティテイの電子署名が付加された構成であり、

前記情報処理装置は、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする請求項２５に記載の情報処理装置。

【請求項２９】前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記情報処理装置は、

前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする請求項２５に記載の情報処理装置。

【請求項３０】コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおいて、コンテンツ利用権限証明書の発行処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

発行済みのコンテンツ利用条件情報を伴うコンテンツ利用条件変更処理要求を受信するステップと、

受信したコンテンツ利用権限証明書の検証処理を実行するステップと、

該検証により前記コンテンツ利用権限証明書の正当性が確認されたことを条件として、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信するステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。特に、暗号化されたコンテンツを配信するシステムにおいて、コンテンツの利用権限情報等を含むコンテンツ利用権限証明書、例えば属性証明書を利用したコンテンツ鍵の配送により、コンテンツの不正利用を防止するとともに、コンテンツ利用権限証明書に基づいて新たな

利用条件または新たなコンテンツに対応するコンテンツ利用権限証明書を発行して、新たなコンテンツ利用を可能としたコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】昨今、音楽データ、画像データ、ゲームプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット、衛星を介した通信他、有線、無線の各種通信網を介して配信するサービスが盛んになってきている。また、ＤＶＤ、ＣＤ、メモリカード等の流通可能な記憶媒体を介したコンテンツ流通も盛んになってきている。これらの流通コンテンツは、ユーザの所有する例えば、ＴＶ、ＰＣ（Personal Computer）、再生専用器、あるいはゲーム機器等において、再生、利用される。

【０００３】通信網を介して配信されるコンテンツは、例えば通信機能を有するセットトップボックスによって受信され、ＴＶ他の再生装置において再生可能なデータに変換されて再生されたり、あるいは通信インタフェースを備えたＴＶ、再生装置、ゲーム機器、ＰＣ等の情報機器によって受信されて再生される。

【０００４】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００５】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。例えば著作権保護の要請されるコンテンツを衛星通信あるいはインターネット通信等を介した配信、あるいはＤＶＤ等のメディアに格納して配布する場合にコンテンツを暗号化して配信または格納し、正規ユーザに対してのみコンテンツ復号に利用可能な復号鍵を配布する。正規ユーザは配布された復号鍵によって暗号化コンテンツの復号を実行し、コンテンツを再生する構成である。

【０００６】暗号化データは、復号鍵を用いた復号化処理によって復号データ（平文）に戻すことができる。データ暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００７】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Data encryption standard）がある。

【０００８】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【０００９】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なる鍵で行なう方式がいわゆる公開鍵暗号方式と呼ばれる方式である。公開鍵暗号方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が生成した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号化処理が可能となる。秘密鍵は、公開鍵を生成した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号方式の代表的なものには、楕円曲線暗号、あるいはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【００１０】

【発明が解決しようとする課題】上記のようなコンテンツ利用管理システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはＤＶＤ、ＣＤ等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツ鍵を正当なユーザにのみ提供する構成が多く採用されている。コンテンツ鍵自体の不正な利用等を防ぐためのコンテンツ鍵を暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を使用可能とする構成が提案されている。

【００１１】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツ鍵の配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツ鍵を暗号化して通信を行なう。

【００１２】しかし、このような認証処理をベースとしてユーザの確認を行なってコンテンツまたはコンテンツ鍵を配信する構成においては、コンテンツ鍵を配信する側で、ユーザ毎のコンテンツ利用権限情報を管理することが必要となる。すなわち、ユーザが正当なコンテンツ利用権限をもつか否かを判定するため、すべてのユーザのコンテンツ利用権限情報をデータベースに格納し、権限情報に基づいて、コンテンツまたはコンテンツ鍵の配布を行なう処理が必要となる。

【００１３】このような処理、すなわちユーザのコンテンツ利用権限の確認処理は、コンテンツを利用するユーザ数が限られた範囲の少数であれば何ら問題ないが、ユーザ数が膨大になると、処理負荷が大きくなり、コンテンツの配信、またはコンテンツ鍵の配信処理の効率を低下させることになる。また、ユーザによっては、コンテンツの利用条件として設定された期間制限、回数制限等の条件をコンテンツの購入後に変更したい場合が発生し得る。

【００１４】本発明は、上述の問題点に鑑みてなされたものであり、ユーザのコンテンツ利用権限を、サービスプロバイダ側でユーザ毎に管理することなく、正当なユーザにおいてのみコンテンツ利用を可能とし、さらに、期間制限、回数制限等、ユーザに対応した様々な利用制限の変更処理、あるいは新たなコンテンツの購入を、購入済のコンテンツに対応する情報に基づいて実行することを可能としたコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムを提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明の第１の側面は、コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有し、前記ユーザデバイスは、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用を行なう構成を有するとともに、前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報の変更処理要求を実行する構成を有し、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツ利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とするコンテンツ利用権限管理システムにある。

【００１６】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記ユーザデバイスは、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であることの判定を条件として、前記暗号化コンテンツ鍵の復号を実行してコンテンツ鍵を取得する構成であることを特徴とする。

【００１７】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記ユーザデバイスは、コンテンツ利用に際して、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、ユーザデバイス内に格納した鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行する構成を有することを特徴とする。

【００１８】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記サービスプロバイダは、ユーザデバイスにおけるコンテンツ利用に際して、該ユーザデバイスから送付済みコンテンツ利用権限証明書を受信し、受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、サービスプロバイダ固有鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行する構成を有することを特徴とする。

【００１９】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報は、コンテンツ利用期間制限情報、コンテンツ利用回数制限情報、利用制限を設けないコンテンツ買い切りの３態様のいずれかであり、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求は、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを含み、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理

として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする。

【００２０】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする。

【００２１】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする。

【００２２】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする。

【００２３】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、属性証明書認証局の発行する属性証明書であり、コンテンツの復号に適用するコンテンツ鍵を暗号化した暗号化コンテンツ鍵を、属性証明書中の属性情報フィールドに格納した構成であることを特徴とする。

【００２４】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、属性証明書認証局の発行する属性証明書であり、属性証明書中の属性情報フィールドに、コンテンツの利用条件を格納した構成であることを特徴とする。

【００２５】さらに、本発明の第２の側面は、コンテンツの利用を行なうユーザデバイスと、購入コンテンツ情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有し、前記ユーザデバイスは、前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、前記サービスプロバイダは、前記ユーザデバイスから受信したコンテンツ利用権限証明書に格納されたコンテンツ情報に基づいて、該コンテンツ情報と同一の集合コンテンツとして識別される同一アルバムに属するコンテンツに対応するコンテンツ利用権限証明書をアップグレードコンテンツ利用権限証明書として生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とするコンテンツ利用権限管理システムにある。

【００２６】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする。

【００２７】さらに、本発明のコンテンツ利用権限管理システムの一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする。

【００２８】さらに、本発明の第３の側面は、コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおけるコンテンツ利用権限管理方法であり、前記ユーザデバイスは、前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報の変更処理要求を実行し、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツ利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とするコンテンツ利

用権限管理方法にある。

【００２９】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記ユーザデバイスは、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であることの判定を条件として、前記暗号化コンテンツ鍵の復号を実行してコンテンツ鍵を取得することを特徴とする。

【００３０】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記ユーザデバイスは、コンテンツ利用に際して、前記サービスプロバイダから受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、ユーザデバイス内に格納した鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行することを特徴とする。

【００３１】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、暗号化コンテンツを復号するためのコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵を格納し、前記サービスプロバイダは、ユーザデバイスにおけるコンテンツ利用に際して、該ユーザデバイスから送付済みコンテンツ利用権限証明書を受信し、受信したコンテンツ利用権限証明書に格納されたコンテンツ利用条件情報に従ったコンテンツ利用であるか否かの判定処理を実行し、判定結果に基づいて、コンテンツ利用条件に従ったコンテンツ利用であるとの判定が得られたことを条件として、サービスプロバイダ固有鍵に基づいて、前記コンテンツ利用権限証明書に格納された暗号化コンテンツ鍵の復号化処理を実行することを特徴とする。

【００３２】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件情報は、コンテンツ利用期間制限情報、コンテンツ利用回数制限情報、利用制限を設けないコンテンツ買い切りの３態様のいずれかであり、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求は、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを含み、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とする。

【００３３】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、前記サービスプロバイダは、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行することを特徴とする。

【００３４】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行することを特徴とする。

【００３５】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行することを特徴とする。

【００３６】さらに、本発明の第４の側面は、コンテンツの利用を行なうユーザデバイスと、購入コンテンツ情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおけるコンテンツ利用権限管理方法であり、前記ユーザデバイスは、前記コンテンツ利用権限証明書を前記サービスプロバイダに送付し、前記サービスプロバイダは、前記ユーザデバイスから受信したコンテンツ利用権限証明書に格納されたコンテンツ情報に基づいて、該コンテンツ情報と同一の集合コンテンツとして識別される同一アルバムに属するコンテンツに対応するコンテン

ツ利用権限証明書をアップグレードコンテンツ利用権限証明書として生成し、ユーザデバイスに対して送信する処理を実行することを特徴とするコンテンツ利用権限管理方法にある。

【００３７】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行することを特徴とする。

【００３８】さらに、本発明のコンテンツ利用権限管理方法の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行するることを特徴とする。

【００３９】さらに、本発明の第５の側面は、コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおいて、コンテンツ利用権限証明書を発行する情報処理装置であり、ユーザデバイスから発行済みのコンテンツ利用条件情報を伴うコンテンツ利用条件変更処理要求を受信し、受信したコンテンツ利用権限証明書の検証処理を実行し、該検証により前記コンテンツ利用権限証明書の正当性が確認されたことを条件として、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする情報処理装置にある。

【００４０】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする。

【００４１】さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ利用権限証明書に格納されたコンテンツ利用条件には、サービスプロバイダにおける利用権限判定処理を必須条件とするオンライン利用処理、または、サービスプロバイダにおける利用権限判定処理を不要とするオフライン利用処理のいずれかを設定した利用条件情報を含み、前記情報処理装置は、前記ユーザデバイスからのコンテンツの利用条件情報の変更処理要求を伴う前記コンテンツ利用権限証明書の受信に応じて、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報の変更処理として、オンライン利用処理とオフライン利用処理間の利用条件情報変更を実行してアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信する処理を実行する構成を有することを特徴とする。

【００４２】さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書の発行エンティティの電子署名が付加された構成であり、前記情報処理装置は、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成であることを特徴とする。

【００４３】さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ利用権限証明書は、該コンテンツ利用権限証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記情報処理装置は、前記コンテンツ利用権限証明書の受信に基づくアップグレードコンテンツ利用権限証明書の生成処理を、前記リンク情報によって取得される公開鍵証明書の検証により、該コンテンツ利用権限証明書の正当性確認を条件として実行する構成であることを特徴とする。

【００４４】さらに、本発明の第６の側面は、コンテンツの利用を行なうユーザデバイスと、コンテンツ利用条件情報を格納したコンテンツ利用権限証明書をユーザデバイスに対して配信するサービスプロバイダとを有するシステムにおいて、コンテンツ利用権限証明書の発行処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、発行済みのコンテンツ利用条件情報を伴うコンテンツ利用条件変更処理要求を受信するステップと、受信したコンテンツ利用権限証明書の検証処理を実行するステップと、該検証により前記コンテンツ利用権限証明書の正当性が確認されたことを条件として、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して送信するステップと、を有することを特徴とするコンピュータ・プログラムにある。

【００４５】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形

式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００４６】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００４７】

【発明の実施の形態】［システム概要］図１に本発明のコンテンツ利用管理システムにおける各エンティテイ、.および各エンティテイの処理の概要を説明する図を示す。

【００４８】ユーザデバイス１０１は、コンテンツを利用する各ユーザの端末であり、具体的には、ＰＣ、ゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置等である。これらの端末には、後段で説明する暗号処理、コンテンツ利用処理を制御する制御手段を備えた耐タンパ構成のセキュリティチップが装着されている。コンテンツ配信エンティテイ（コンテンツディストリビュータ）としてのサービスプロバイダ（ＳＰ－ＣＤ）１０２、その他のエンティテイとユーザデバイス１０１間で実行されるデータ転送等におけるユーザデバイス１０１側のセキュアな処理の多くは、セキュリティチップ内で制御、実行される。

【００４９】サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２は、セキュリティチップを持つユーザデバイス１０１に対してコンテンツを提供するサービスプロバイダである。コンテンツクリエータ１０３は、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２に対してサービスに供するためのコンテンツを提供する。ユーザデバイス製造者（Manufacturer）１０４は、ユーザデバイス１０１を製造するエンティテイである。

【００５０】サポートセンタ１０５は、ユーザデバイス１０１に装着されたユーザデバイスでの様々な処理に対するサポートを実行するセンタであり、例えばユーザが認証情報として利用するパスワードを忘れた場合のパスワードのリカバリ処理、あるいはユーザデバイスが生成したコンテンツのバックアップデータを利用したリストア（復旧）処理など、ユーザデバイスに対する様々なサポート処理を実行する。認証局（ＣＡ：Certification Authority）１０６は各エンティテイに対して公開鍵証明書(ＰＫＣ：Public Key Certificate)を発行する。

【００５１】なお、ユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２、コンテンツクリエータ１０３、ユーザデバイス製造者（Manufacturer）１０４、サポートセンタ１０５、認証局（ＣＡ：Certification Authority）１０６、各エンティテイの数は任意である。特に、図１において、認証局（ＣＡ：Certification Authority）１０６を１つのみ示してあるが、認証局は、各エンティテイでの処理に応じて必要となる公開鍵証明書を発行する複数の認証局が存在してよい。

【００５２】ユーザデバイス１０１は、衛星通信、インターネット通信、あるいはその他、有線、無線のデータ通信ネットワークを介してサービスプロバイダ（コンテンツディストリビュータ）１０２から暗号化されたコンテンツを受信し、コンテンツを利用する。暗号化コンテンツを復号するための鍵：コンテンツ鍵：Ｋｃは暗号化されてコンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（ＡＣ：Attribute Certificate）１１０に格納されており、ユーザ端末１０１がコンテンツを復号して利用するためには、サービスプロバイダ（コンテンツディストリビュータ）１０２から属性証明書（ＡＣ：Attribute Certificate）１１０を受領し、セキュリティチップを持つユーザデバイスにおいて属性証明書から鍵を取り出して復号することが必要となる。

【００５３】コンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（ＡＣ：Attribute Certificate）１１０には、暗号化されたコンテンツ鍵：Ｋｃの他に、コンテンツの利用制限回数や利用期限など、コンテンツの利用制限情報が記録されており、ユーザデバイス１０１は、コンテンツ利用権限証明書としての属性証明書（ＡＣ）１１０に記録されたコンテンツ利用制限に従ったコンテンツの利用が可能となる。

【００５４】なお、以下、実施例の説明では、属性証明書（ＡＣ：Attribute Certificate）１１０にコンテンツの利用情報、暗号化コンテンツ鍵を格納した構成として説明するが、コンテンツの利用情報、暗号化コンテンツ鍵を格納した証明書は、いわゆる規定に従った属性証明書（ＡＣ）に限らず、任意のデータフォーマットの証明書として構成可能である。すなわちコンテンツの利用権限を証明するデータを格納し、データ改竄検証のための発行エンティテイの署名データが付加された構成であれば、任意のデータ形式のコンテンツ利用権限証明書が利用可能である。

【００５５】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシ

ュ型の形態(プッシュ型モデル)のいずれの形態も可能である。

【００５６】図１で示す各エンティテイ中、認証局１０６以外のエンティテイ、すなわちユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２、コンテンツクリエータ１０３、およびユーザデバイス製造者（Manufacturer）１０４、サポートセンタ１０５のエンティテイは、所定のルールに従ってコンテンツ利用、コンテンツ配信を可能とするため、各エンティテイでの処理を所定のルールに従って実行する。このルールを設定し、管理するエンティテイとして図示しないシステムホルダ（ＳＨ:System Holder）がある。図１の１０１～１０５の各エンティテイは、システムホルダ（ＳＨ）の設定したコンテンツ利用インフラ、ルールの下で各エンティテイでの処理を実行する。

【００５７】例えばユーザデバイス製造者（Manufacturer）１０４は、製造するユーザデバイス内の耐タンパ構成を持つセキュリティチップ内に、コンテンツ配信において適用するデバイス識別子（ＩＤ）、および各種の暗号処理鍵を格納する。ユーザデバイス１０１、サービスプロバイダ（コンテンツディストリビュータ）１０２、コンテンツクリエータ（ＣＣ）１０３、サポートセンタ１０５間でのコンテンツ転送、属性証明書の転送、その他のデータ転送処理においては、システムホルダ（ＳＨ）の設定したルールに基づいて、例えば相互認証処理、データ暗号化処理を実行する。

【００５８】また、ユーザデバイス１０１におけるコンテンツ利用に際しては、属性証明書に記録された利用制限を遵守したコンテンツ利用を実行する。例えば回数制限の設定されたコンテンツの利用に際してデバイス内のセキュリティチップの制御部の制御の下に、コンテンツ利用可能回数を係数するカウンタを更新する処理等を実行する。このような各エンティテイでの処理のルールを規定したプラットホームを構築し、管理するエンティテイがシステムホルダ（ＳＨ）である。

【００５９】［公開鍵証明書，属性証明書］図１の構成において利用される公開鍵証明書、属性証明書について、その概要を説明する。

【００６０】（公開鍵証明書（ＰＫＣ））公開鍵証明書について図２，図３、図４を用いて説明する。公開鍵証明書は、認証局（ＣＡ：Certification Authority）が発行する証明書であり、ユーザ、各エンティテイが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【００６１】公開鍵証明書のフォーマット例を図２～図４に示す。これは、公開鍵証明書フォーマットＩＴＵ－Ｔ　Ｘ．５０９に準拠した例である。

【００６２】バージョン（version）は、証明書フォーマットのバージョンを示す。シリアルナンバ（Serial Number）は、公開鍵証明書発行局（ＣＡ）によって設定される公開鍵証明書のシリアルナンバである。シグネチャ（Signature）は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（ＩＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。サブジェクト公開鍵情報(subject Public Key Info)は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

【００６３】証明局鍵識別子（authority Key Identifier－key Identifier、authority Cert Issuer、authority Cert Serial Number）は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（０）ディジタル署名用、（１）否認防止用、（２）鍵の暗号化用、（３）メッセージの暗号化用、（４）共通鍵配送用、（５）認証の署名確認用、（６）失効リストの署名確認用の各使用目的が設定される。秘密鍵有効期限(private Key Usage Period)は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。認証局ポリシー（certificate Policies）は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えばＩＳＯ／ＩＥＣ９３８４－１に準拠したポリシーＩＤ、認証基準である。ポリシー・マッピング（policy Mapping）は、認証パス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局（ＣＡ）証明書にのみ必要となる。サブジェクト別名（subject Alt Name）は、証明書所有者の別名を記録するフィールドである。発行者別名（issuer Alt Name）は、証明書発行者の別名を記録するフィールドである。サブジェクト・ディレクトリ・アトリビュート（subject Directory Attribute）は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。基本制約（basic Constraint）は、証明対象の公開鍵が認証局（ＣＡ）の署名用か、証明書所有者のものかを区別するためのフィールドである。許容サブツリー制約名（name Constraints permitted Subtrees）は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。制約ポリシー（policy Constraints）は、認証パス中のポリシーの関

係の制限情報を格納するフィールドである。ＣＲＬ参照ポイント（Certificate Revocation List Distribution Points）は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。署名アルゴリズム（Signature Algotithm）は、証明書の署名付けに用いるアルゴリズムを格納するフィールドである。署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【００６４】認証局は、図２～図４に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト（Revocation List）の作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【００６５】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００６６】（属性証明書（ＡＣ））属性証明書について図５を用いて説明する。属性証明書には大きく分けて２つの種類があり、１つは、コンテンツの利用権といった権利や権限に関する所有者の属性情報を含む証明書である。もう１つは、サービスプロバイダ（ＳＰ）用領域確保または削除用属性証明書（ＡＣ）であり、ユーザデバイス内のメモリにサービスプロバイダ（ＳＰ）用情報格納領域を確保または削除する場合の領域確保または削除の許諾情報を含む属性証明書（ＡＣ）である。

【００６７】属性証明書フォーマットはITU-T X.509で規定されており，IETF PKIX WGでProfileを策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性証明書認証局(Attribute Certificate Authority)の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

【００６８】本発明の構成においては、属性証明書（ＡＣ）の発行管理を行なう属性証明書認証局(Attribute Certificate Authority)は、サービスプロバイダ（コンテンツディストリビュータ）（ＳＰ－ＣＤ）１０２が兼務することが可能である。別の構成としてもよい。属性証明書は常に公開鍵証明書と関連づけて利用する。すなわち所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかのみを示すものが属性証明書である。属性証明書の検証にあたっては，当該証明書の署名検証を行った後、それに関連づけられている公開鍵証明書の検証も行う。

【００６９】なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局（ＣＡ）が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の公開鍵証明書発行局（ＣＡ－Ｌｏｗ）に対して上位の公開鍵証明書発行局（ＣＡ－Ｈｉｇｈ）が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なうことを意味する。

【００７０】属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければならない。本認証システムにおいては、コンテンツに対する利用権限の他に、コンテンツを復号するためのコンテンツ鍵を属性証明書に埋め込んでおく構成であるので、正当なコンテンツ利用権限のあるユーザデバイスは、正当な属性証明書を受領することにより、コンテンツを利用可能である。

【００７１】図５に示す属性証明書の構成について説明する。証明書のバージョン番号は、証明書フォーマットのバージョンを示す。ＡＣ保持者の公開鍵証明書情報、これは属性証明書（ＡＣ）の発行者に対応する公開鍵証明書（ＰＫＣ）に関する情報であり、ＰＫＣ発行者名、ＰＫＣシリアル番号、ＰＫＣ発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性証明書認証局（ＡＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。属性情報フィールドは、属性証明書の利用形態に応じて、（１）メモリ領域確保、削除情報、または、（２）コンテンツ利用条件関連情報のいずれかが格納される。コンテンツ利用条件関連情報には、暗号化されたコンテンツ鍵を含む。

【００７２】（１）メモリ領域確保、削除情報は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設

定、または削除処理を目的として発行される属性証明書に記録される。記録情報は、例えば以下の情報である。
サービスプロバイダ識別子（ＩＤ）
サービスプロバイダ・ネーム
処理：メモリ領域確保、メモリ領域削除のいずれか
領域サイズ：メモリ領域のサイズ
【００７３】サービスプロバイダは、上記各項目を属性情報フィールドに格納した属性証明書をユーザデバイスに対して送付し、ユーザデバイスは属性証明書の検証の後、自己のセキュリティチップ内のメモリに、受信した属性証明書の属性情報フィールドの記録に従ったメモリ領域の確保処理、または確保済みのメモリ領域の削除処理を実行する。
【００７４】（２）コンテンツ利用条件関連情報は、サービスプロバイダの提供するコンテンツに対応して発行される属性証明書の属性情報フィールドに格納する情報であり、コンテンツの利用制限回数、利用期限等の様々な利用条件を含み、さらにコンテンツを暗号化したコンテンツ鍵の暗号化データを含む。記録情報は、例えば以下の情報である。
サービスプロバイダ識別子（ＩＤ）
サービスプロバイダ・ネーム
アプリケーション識別子（ＩＤ）：コンテンツの識別情報である。
条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報である。
有効期限：期間制限の場合の有効期限情報
利用制限回数：回数制限の場合の利用可能回数
支払条件：コンテンツの対価の支払条件を記録
コンテンツ鍵：暗号化されたコンテンツ鍵を暗号化アルゴリズム情報とともに格納
【００７５】コンテンツの利用態様には、上記条件フィールドに記載のように、（１）オンライン利用か、（２）オフライン利用かの区別と、（ａ）コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとする態様、（ｂ）期間制限を設けてコンテンツの利用期間を設定した態様、（ｃ）回数制限を設けてコンテンツの利用回数を制限した態様の各態様がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツの利用が実行される。これらの具体的な処理態様については、後段で説明する。
【００７６】また、暗号化コンテンツの復号鍵として適用するコンテンツ鍵：Ｋｃを暗号化した暗号化コンテンツ鍵が格納される。コンテンツ鍵：Ｋｃの暗号化処理に直接あるいは間接的に適用する鍵の主な種類は以下に示す通りである。
（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ、（公開鍵方式）
（ｂ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵方式）
（ｃ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋ
（ｄ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇ
これらの鍵を適用した処理については後段で詳細に説明する。
【００７７】属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者である属性証明書認証局（ＡＡ）によって署名が施される。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者（ＡＡ）の秘密鍵を用いて生成したデータである。
【００７８】［セキュリティチップ構成］次にコンテンツを利用する情報処理装置としてのユーザデバイス内に構成されるセキュリティチップの構成について、図６を参照しながら説明する。なお、ユーザデバイスは、データ処理手段としてのＣＰＵ、通信機能を備えたＰＣ、ゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置等によって構成されるものであり、これらのユーザデバイスの中に耐タンパ構造を持つセキュリティチップが実装されることになる。ユーザデバイス自体の構成例は本明細書の末尾において説明する。セキュリティチップを持つユーザデバイスは、図１におけるユーザデバイス製造者１０４において製造される。
【００７９】図６に示すように、ユーザデバイス２００には、セキュリティチップ２１０が、ユーザデバイス側制御部２２１に対して、相互にデータ転送可能な構成として内蔵される。セキュリティチップ２１０は、プログラム実行機能、演算処理機能を持つＣＰＵ（Central Processing Unit）２０１を有し、データ通信用のインタフェース機能を持つ通信インタフェース２０２、ＣＰＵ２０１によって実行される各種プログラム、例えば暗号処理プログラム、デバイスの製造時に格納されるマスター鍵：Ｋｍなどを記憶するＲＯＭ（Read Only Memory）２０３、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するＲＡＭ（Random Access Memory）２０４、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部２０５、前述したサービスプロバイダ毎の情報、各種鍵データを含むデバイスの固有情報を格納した例えばＥＥＰＲＯＭ(Ele

ctrically Erasable Programmable ROM)によって構成されるメモリ部２０６を有する。これら格納情報の詳細については後述する。

【００８０】ユーザデバイス２００は、暗号化コンテンツ等を格納する領域としてのＥＥＰＲＯＭ、ハードディスク等によって構成される外部メモリ部２２２を有する。外部メモリ部２２２は、公開鍵証明書、属性証明書の格納領域としても利用可能であり、また後段で説明するコンテンツの利用回数管理ファイルの格納領域としても利用される。

【００８１】セキュリティチップを搭載したユーザデバイスが、外部エンティテイ、例えばサービスプロバイダと接続し、データ転送処理を実行する場合には、必要に応じて、セキュリティチップ２１０と、外部エンティテイ間の相互認証が行われ、また転送データの暗号化が行なわれる。これらの処理の詳細については、後段で詳述する。

【００８２】ユーザデバイスのセキュリティチップでの処理対象となるデータ例を図７に示す。これらの多くは、不揮発性メモリの一形態であるフラッシュメモリ等のＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６に格納されるが、製造時に格納し、書き換え不可能とするデータ、例えばマスター鍵：Ｋｍは、ＲＯＭ（Read Only Memory）２０３に格納される。公開鍵証明書、属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

【００８３】各データについて説明する。

公開鍵証明書（ＰＫＣ）：公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局によりディジタル署名されている。ユーザデバイスには、前述した階層構成の最上位認証局（ルートＣＡ）の公開鍵証明書、ユーザデバイスに登録されたサービスプロバイダ、すなわち、ユーザデバイス内にメモリ領域が確保されているサービスプロバイダの公開鍵証明書、さらに、パスワード復帰処理等のサポートを実行するサポートセンタの公開鍵証明書を格納する。

【００８４】属性証明書（ＡＣ）：公開鍵証明書が証明書利用者（所有者）の“本人性”を示すのに対し、属性証明書は証明書利用者の利用権限を示すものである。利用者は属性証明書を提示することにより、属性証明書に記載された権利・権限に基づいて、アプリケーションの利用や、領域の確保などが行えるようになる。以下に、属性証明書の種類を示し、それぞれの果たす役割を示す。

【００８５】（ａ）アプリケーション利用管理用属性証明書（ＡＣ）：アプリケーションとは、一般に言われるコンテンツを広い意味で使用した表現であり、アプリケーションの種類としては、ゲーム、音楽、映画、金融情報等の各種アプリケーションがある。アプリケーション利用管理用属性証明書（ＡＣ）では、アプリケーションの利用権限に関しての記述があり、属性証明書（ＡＣ）をサービスプロバイダ（ＳＰ）に対して提示して検証、もしくは、ローカルで検証することにより、属性証明書（ＡＣ）に記述された利用権限範囲内でのアプリケーションの利用許諾が得られる。アプリケーションの利用権限に関する記述としては、アプリケーションのオンライン利用が可能であるかオフライン利用が可能であるか、さらに、オンライン利用可能なコンテンツの場合には、利用期間制限、利用回数制限情報があり、オフライン利用可能なコンテンツの場合には、利用回数制限、買い切りを示す記述がある。

【００８６】（ｂ）サービスプロバイダ（ＳＰ）用メモリ領域管理（確保）用属性証明書（ＡＣ）：ユーザデバイスにサービスプロバイダ（ＳＰ）を登録する場合、ＳＰに関する情報格納領域をユーザデバイス内に確保する必要がある。この時の領域確保の許諾情報を属性証明書（ＡＣ）に格納し、ユーザデバイスでは、属性証明書（ＡＣ）に格納された情報に従って、ユーザデバイス内にＳＰ用の領域を確保する。

【００８７】（ｃ）サービスプロバイダ（ＳＰ）用メモリ領域管理（削除）用属性証明書（ＡＣ）：ユーザデバイス内に確保したＳＰ用領域の削除の許諾情報を格納した属性証明書（ＡＣ）である。ユーザデバイスでは、属性証明書（ＡＣ）に格納された情報に従って、ユーザデバイス内のＳＰ用の領域の削除処理を実行する。

【００８８】鍵データ：鍵データとしては、デバイスに対して設定される公開鍵、秘密鍵のペア、コンテンツ等のデータ保存の際の暗号処理用鍵として用いられるストレージ鍵、さらに、乱数生成用鍵、相互認証用鍵等が格納される。

【００８９】ストレージ鍵は、デバイスに保存するコンテンツ鍵の暗号化または復号化処理の少なくともいずれかに適用する鍵である。ストレージ鍵には、デバイス対応ストレージ鍵、サービスプロバイダ対応ストレージ鍵があり、サービスプロバイダ対応ストレージ鍵は、デバイスに登録された個々のサービスプロバイダ毎に各サービスプロバイダ管理領域内に格納される鍵であり、対応するサービスプロバイダの提供するコンテンツ鍵に対応して適用される。デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。これらの鍵を適用した処理の詳細については後段で説明する。

【００９０】識別情報：識別情報としては、ユーザデバイス自身の識別子としてのデバイスＩＤ、ユーザデバイスに登録したサービスプロバイダ（ＳＰ）の識別子とし

てのサービスプロバイダＩＤ、ユーザデバイスを利用するユーザに付与されたユーザＩＤ、なお、ユーザＩＤはサービスプロバイダ等、外部エンティテイ毎に異なるユーザＩＤが付与可能である。アプリケーションＩＤは、サービスプロバイダ（ＳＰ）によって提供されるサービス、コンテンツに対応する識別情報としてのＩＤである。

【００９１】その他：ユーザデバイスには、さらに、認証情報として、ユーザデバイス内に登録したサービスプロバイダ（ＳＰ）情報の利用許諾を得るための認証情報（例えばパスワード）が格納される。パスワードを入力することにより、ユーザデバイス内に登録したサービスプロバイダ（ＳＰ）情報の取得が可能となり、情報取得後、サービスプロバイダの提供するアプリケーション、コンテンツの利用が許可される。認証情報（パスワード）を忘れた場合には、マスターパスワードを用いて認証情報（パスワード）の初期化（リセット）処理が可能である。

【００９２】さらに乱数生成用のシード情報が格納される。乱数は、認証処理、暗号処理等の際に、例えばＡＮＳＩ　Ｘ９．１７に従って生成する。

【００９３】さらに、コンテンツ利用回数情報、あるいはコンテンツ利用回数情報に基づいて算出されるハッシュ値が格納される。これは、アプリケーション、コンテンツに対応する属性証明書に格納された利用回数制限内でのコンテンツ利用を厳格に実行するために必要となる情報であり、コンテンツに対応する属性証明書の識別情報としてのアプリケーションＩＤ、属性証明書のシリアル番号、コンテンツの利用制限回数を保存する。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【００９４】［ユーザデバイス内のメモリ構成］不揮発性メモリの一形態であるフラッシュメモリ等のＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６には、上述した様々なデータの少なくとも一部が格納されるが、これらは、メモリ部２０６領域に分割管理された３つの領域、すなわち、（１）デバイス管理領域、（２）システム管理領域、（３）サービス・プロバイダ管理領域に区分されて格納される。以下、これらの各領域毎の格納データについて説明する。

【００９５】（１）デバイス管理領域

デバイス管理領域は、デバイス固有のシステムに依存しない情報が保持されている。この領域はデバイス製造時に、最初に領域が確保され、不揮発性メモリの先頭の複数ブロックを占める領域である。デバイス管理領域では、少なくとも以下のデータを保持・管理する。

デバイスＩＤ

乱数生成用シード

乱数生成用暗号鍵

相互認証鍵

デバイス対応ストレージ鍵

【００９６】相互認証鍵は、セキュリティチップ内のデータをセキュリティチップ外部に出力する場合等に出力先となるエンティテイとの認証用の鍵である。なお、エンティテイは、セキュリティチップを装着した例えばゲーム端末、ＤＶＤ，ＣＤ等の再生装置、記録再生装置であるユーザデバイスも含む。セキュリティチップと、セキュリティチップを持つユーザデバイス間でのデータ転送、さらにはユーザデバイスを介した外部のサービスプロバイダとのデータ通信時などに相互認証鍵を適用した相互認証処理が実行される。相互認証の成立を条件として、相互認証時に生成したセッション鍵で暗号化してセキュリティチップ内部と外部間のデータ転送が実行される。

【００９７】デバイス対応ストレージ鍵は、セキュリティチップ内部のデータを外部に保持する場合に、データを暗号化し、閲覧・改竄を防ぐための鍵である。デバイス・ストレージ鍵は、公開鍵系でも共通鍵系でもどちらでもよい。乱数生成用シードは、擬似乱数を算術演算により求める際に、初期シードとして用いるデータである。乱数生成用暗号鍵を用いて擬似乱数を算術演算して乱数を生成する。

【００９８】共通鍵系デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。グローバル共通鍵については、後段で詳細に説明する。

【００９９】（２）システム管理領域

システム管理領域は、デバイス管理領域と同様にメモリ領域に確保される。システム管理領域では、以下のデータを保持・管理する。

ルート認証局（ＣＡ）公開鍵証明書

デバイス公開鍵証明書

デバイス秘密鍵

【０１００】ルート認証局（ＣＡ）公開鍵証明書は、セキュリティチップ内の認証系すべての根源となる証明書で、他の証明書の署名検証を辿って、前述の連鎖検証を行なうと、最後にはルート認証局（ＣＡ）の公開鍵証明書に辿り着くことになる。

【０１０１】デバイス公開鍵証明書は、サービスプロバイダとの相互認証時に用いる公開鍵証明書である。デバイス秘密鍵を外部で生成し、インポートする場合には、デバイス公開鍵証明書も同時に生成される。デバイス側でデバイス秘密鍵・公開鍵を生成する場合には、デバイス内でデバイス秘密鍵・公開鍵が生成された後に、デバイス公開鍵がデバイスから読み出され、デバイス公開鍵

証明書の発行処理を行ない、発行されたデバイス公開鍵証明書のインポートが行われる。

【０１０２】デバイス秘密鍵は、データに対して署名付けおよび認証するための鍵である。秘密鍵は、公開鍵とペアで生成されるが、予め外部で生成して、デバイスにセキュアにインポートする構成とするか、デバイス内部で生成し、決して外部に出さない構成とするかのいずれかの構成とする。

【０１０３】（３）サービスプロバイダ管理領域

サービスプロバイダ（ＳＰ）管理領域は、サービスプロバイダ（ＳＰ）管理テーブルとサービスプロバイダ（ＳＰ）管理情報とからなる。サービスプロバイダ（ＳＰ）管理テーブルは、サービスプロバイダ（ＳＰ）管理領域内で各サービスプロバイダ（ＳＰ）情報の所在を示すためのテーブルでありサービスプロバイダの識別子に対応させてメモリの各サービスプロバイダ（ＳＰ）情報の格納位置情報を持つ。

【０１０４】なお、サービスプロバイダ（ＳＰ）管理領域には、ユーザデバイスがサービスプロバイダ（ＳＰ）毎に会員登録を行うことにより、サービスプロバイダ（ＳＰ）毎の領域がデバイス内のメモリ領域に確保される。なお、領域確保あるいは削除処理は、属性証明書の記述に基づいて実行される。サービスプロバイダ（ＳＰ）管理領域には、以下の情報を保持する。

【０１０５】サービスプロバイダ（ＳＰ）対応秘密鍵

サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）

サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）

外部管理情報のハッシュ値

コンテンツ利用回数管理データ

認証情報

ユーザ情報

【０１０６】サービスプロバイダ（ＳＰ）対応秘密鍵は、登録サービスプロバイダ（ＳＰ）毎に対応して生成した登録サービスプロバイダ（ＳＰ）との相互認証処理または暗号化データ転送処理等に適用する公開鍵と秘密鍵のペアの秘密鍵である。登録サービスプロバイダ（ＳＰ）と、セキュリティチップとが相互認証する場合に必要とする鍵である。

【０１０７】サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵である。暗号化コンテンツ鍵は、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵によってサービスプロバイダにおいて暗号化されて属性証明書（ＡＣ）に格納されてユーザデバイスに送信され、ユーザデバイスのセキュリティチップ内でサービスプロバイダ（ＳＰ）対応ストレージ秘密鍵で復号してコンテンツ鍵の取得が可能となる。

【０１０８】サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵であり、暗号化、復号化処理に共通に適用可能な鍵である。なお、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵（公開鍵方式）と、サービスプロバイダ（ＳＰ）対応ストレージ鍵（共通鍵方式）は、いずれか一方のみを格納し適用する構成としてもよい。。

【０１０９】外部管理情報のハッシュ（Ｈａｓｈ）値は、セキュリティチップ内部で管理するには大きすぎるデータを外部メモリの特定領域に出し、その領域のハッシュ値をセキュリティチップ内で管理することにより、改竄ができないようにするものである。例えば、コンテンツの回数利用制限をかける場合に、残回数などがハッシュ値による管理対象となる。回数管理コンテンツの場合、回数情報の閲覧自体は問題ないが、改竄は防がなくてはならない。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【０１１０】コンテンツ利用回数管理データ

アプリケーション（コンテンツ）の利用可能回数をセキュリティチップがローカルで管理する場合がある。この時、セキュリティチップ内部では、アプリケーションＩＤ、属性証明書（ＡＣ）のシリアル、利用可能回数とを保持・管理する。コンテンツ利用回数管理データの管理処理については、後段で詳細に説明する。

【０１１１】認証情報

認証情報とは、サービスプロバイダ（ＳＰ）管理領域で管理される管理情報を保護する目的の情報である。ユーザはサービスプロバイダ（ＳＰ）接続時にはサービスプロバイダ（ＳＰ）との相互認証が必要となるが、相互認証に必要な情報は、サービスプロバイダ（ＳＰ）管理領域に格納される。この管理領域から必要情報を取得するために用いるのが認証情報である。認証情報は具体的には、例えばパスワードである。認証情報（パスワード）をユーザが忘れた場合には、サービスプロバイダ（ＳＰ）管理領域の管理情報の利用許諾が得られなくなる。この場合には、マスター・パスワードを入力することにより認証情報自体のリセット、または変更を行うことができる。これらの処理構成については、後段で詳細に説明する。

【０１１２】ユーザ情報

ユーザ情報は、サービスプロバイダ（ＳＰ）により割り

振られたユーザＩＤなどのユーザ固有情報である。

【０１１３】［パスワード管理］以下、図１に示すユーザデバイス１０１が、サービスプロバイダ（コンテンツディストリビュータ）１０２の提供するコンテンツを受領し、属性証明書に従った利用制限の下にコンテンツを利用する処理、およびコンテンツ利用に際して必要となる各種処理の詳細について説明する。まず、コンテンツを提供するサービスプロバイダに関する情報を格納したユーザデバイス内のメモリ領域のサービスプロバイダ管理領域へのアクセス制御用の認証情報（パスワード）について説明する。

【０１１４】（１）認証情報（パスワード）登録処理

ユーザデバイスを購入したユーザがシステムホルダの管理下にある様々なサービスプロバイダからコンテンツを購入する処理、あるいは購入したコンテンツを利用する処理を行なうためには、ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域を設定し、このサービスプロバイダ管理領域にサービスプロバイダ毎の管理情報を格納する処理が必要となる。ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域の設定されたサービスプロバイダを、以下登録サービスプロバイダと呼ぶ。サービスプロバイダ管理領域の設定には、前述の属性証明書を適用し、ユーザデバイスがサービスプロバイダから受信した属性証明書に基づいて、ユーザデバイス内のメモリ領域に属性証明書の記録に従ったサービスプロバイダ管理領域の設定処理を実行する。

【０１１５】サービスプロバイダ管理領域を持つ登録サービスプロバイダに対して、ユーザデバイスがアクセスしてコンテンツの購入、あるいは利用を行なうためには、先ず、ユーザデバイス内のサービスプロバイダ管理領域内の情報を取得することが必要となる。サービスプロバイダ管理領域には、ユーザデバイスとサービスプロバイダ間の相互認証処理に必要な情報が格納されており、これらの情報を取得してサービスプロバイダとの相互認証を行なうことが必要となるからである。

【０１１６】このサービスプロバイダ管理領域にアクセスするためにユーザは各登録サービスプロバイダ毎に設定される認証情報(パスワード)を、ユーザデバイスの入力手段を介して入力することが必要となる。なお、以下の説明において、「サービスプロバイダ毎に」との記述は、「各登録サービス毎かつ各ユーザ毎」と同義である。セキュリティチップ側で入力パスワードと登録パスワードの一致検証を行ない、一致した場合に限り、セキュリティチップ内のメモリに形成されたサービスプロバイダ管理領域内の情報取得が可能となり、その後のサービスプロバイダとの相互認証処理、へのアクセスが可能となる。

【０１１７】認証情報（パスワード）は、ユーザデバイスに登録されたサービスプロバイダ毎に設定される。これらのパスワードの初期登録は、ユーザ自身が実行する。パスワードの初期登録処理について、図８を参照して説明する。図８のシーケンス図において、左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスにおけるユーザインタフェース側処理である。

【０１１８】まず、（１）パスワード登録対象となる対応するサービスプロバイダを指定して認証情報（パスワード）初期登録処理開始要求をユーザが入力する。

（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダが、セキュリティチップ内のメモリにすでに管理領域を設定済みの登録サービスプロバイダであり、パスワード設定されていない状態であるか等のステータス確認処理を行ない、これらが確認された場合に、（３）認証情報（パスワード）初期登録処理を許可する。

【０１１９】次に、ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）パスワードを入力し、（５）セキュリティチップの制御部は入力された認証情報（パスワード）をテンポラリにメモリに保持し、（６）同一パスワードの再入力要求を行ない、

（７）ユーザにより認証情報（パスワード）の再入力がなされると、（８）セキュリティチップの制御部は再入力認証情報（パスワード）とテンポラリにメモリに保持してある認証情報（パスワード）の照合を実行し、照合が成立した場合には、（９）認証情報（パスワード）の書き込み処理を実行し、（１０）書き込み結果をユーザに通知し、ＯＫなら終了する。（１１）ＮＧの場合は、（１）の処理に戻る。

【０１２０】（２）認証情報（パスワード）変更処理

図９および図１０にパスワードの変更処理のシーケンス図を示す。パスワード変更は、登録済みパスワードを用いた変更処理（通常時）と、マスターパスワードを用いた変更処理（緊急時）の２つの処理態様がある。

【０１２１】まず、図９のシーケンス図に基づいて、通常時のパスワード変更処理、すなわち、登録済みパスワードを用いた変更処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスのユーザインタフェース側処理である。

【０１２２】まず、（１）パスワード変更処理対象となる対応するサービスプロバイダを指定して認証情報（パスワード）変更処理開始要求をユーザが入力する。

（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ（ＳＰ）であり、パスワードの設定されたＳＰであるか等のステータス確認を処理を行ない、これらが確認されたことを条件として、（３）登録済みの認証情報（パスワード）入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）登録済みパスワードを入力し、

（５）セキュリティチップの制御部は入力を確認する

と、サービスプロバイダ管理領域に書き込まれている登録認証情報（パスワード）との照合処理を実行する。

【０１２３】照合が成立すると、（６）変更処理許可を通知する。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（７）新たな認証情報（パスワード）を入力し、（８）セキュリティチップの制御部は入力された認証情報（パスワード）をテンポラリにメモリに保持し、（９）同一パスワードの再入力要求を行ない、（１０）ユーザにより認証情報（パスワード）の再入力がなされると、（１１）セキュリティチップの制御部は再入力認証情報（パスワード）とテンポラリにメモリに保持してある認証情報（パスワード）の照合を実行し、照合が成立した場合には、（１２）認証情報（パスワード）の書き込み処理を実行し、（１３）書き込み結果をユーザに通知し、ＯＫなら終了する。（１４）ＮＧの場合は、（１）の処理に戻る。

【０１２４】（３）マスターパスワードを用いた認証情報（パスワード）リセット処理

次に、図１０のシーケンス図に基づいて、緊急時のパスワード変更処理等において実行されるマスターパスワードを用いた認証情報（パスワード）リセット処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスを装着した端末におけるユーザインタフェース側処理である。

【０１２５】まず、（１）パスワード変更処理対象となる対応するサービスプロバイダを指定して認証情報（パスワード）リセット処理開始要求をユーザが入力する。（２）セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ（ＳＰ）であり、パスワードの設定されたＳＰであるか等のステータス確認を処理を行ない、これらの条件を満足する場合に、（３）マスターパスワード入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、（４）マスターパスワードを入力し、（５）セキュリティチップの制御部は入力されたマスターパスワードの照合処理を実行し、正しいマスターパスワードの入力であるか否かを判定し、検証の結果、正しいマスターパスワード入力であると判定すると、（６）サービスプロバイダ管理領域に書き込まれている登録認証情報（パスワード）の初期化、すなわち登録済み認証情報（パスワード）のリセット処理を実行する。

【０１２６】セキュリティチップの制御部は、リセット処理の後、（７）処理結果通知をユーザに通知し、ＯＫであれば、例えば、ユーザは前述の認証情報（パスワード）登録処理を実行する。これらの処理は、先に図８を参照して説明した処理と同様であるので説明を省略する。（８）リセット処理結果がＮＧの場合は、（１）の処理に戻る。

【０１２７】図１０の処理シーケンスを用いて説明したように、マスターパスワードは、各登録サービスプロバイダについて登録済みの認証情報(パスワード)の初期化処理、すなわちリセットする際に適用される。マスターパスワードを用いた認証情報初期化（リセット）処理は、セキュリティチップに登録されたサービスプロバイダすべての認証情報に対して有効である。

【０１２８】図１１にマスターパスワードと各登録サービスプロバイダの認証情報（パスワード）との関係図を示す。図１１に示すようにマスターパスワードは、各サービスプロバイダ対応認証情報に対する上位パスワードとして存在し、マスターパスワードの入力により、各各登録サービスプロバイダの認証情報（パスワード）の初期化（リセット）が実行され、新たな認証情報を各登録サービスプロバイダの認証情報（パスワード）として再登録することが可能となる。

【０１２９】マスターパスワードは、図１２に示すように、ユーザデバイスの購入時に例えばプリントされた用紙がデバイスに添付されて配布される。マスターパスワードはデバイスの製造時に工場で書き込まれるが、ユーザによるマスターパスワードのデバイスからの読み出しはできない構成となっている。マスターパスワードは、デバイスに固有の識別子であるデバイスＩＤと、マスターキーに基づいて生成される。マスターキーは情報処理装置個々または一群の情報処理装置に対応して設定されるキーである。

【０１３０】マスターパスワードをユーザが忘れた場合には、サポートセンターへの登録を条件としてマスターパスワードの再発行処理が可能となる。図１３にサポートセンタへのユーザ登録処理および、マスターパスワードの再発行処理シーケンス図を示す。

【０１３１】図１３の上段が、サポートセンタに対するユーザ登録処理シーケンス図を示す。ユーザは購入デバイスに添付された登録用紙の郵送、あるいはデバイスを設定した端末を介してサポートセンタに接続してユーザ登録を行なうことができる。ユーザ登録は、ユーザ住所、電話番号、デバイスのＩＤ等のデータをサポートセンタに登録する処理として実行され、サポートセンタにおいてユーザ登録が完了すると、ユーザ登録完了通知がサポートセンタからユーザに送付または送信される。

【０１３２】図１３の下段が、ユーザがマスターパスワードを忘れた場合に、ユーザと、サポートセンタ間で実行されるマスターパスワード再発行処理のシーケンスである。ユーザは、デバイスＩＤを伴うユーザ情報データとともに、マスターパスワードの再発行要求をサポートセンタに対して送信し、サポートセンタが要求を受信すると、サポートセンタは、ユーザ情報、ユーザＩＤが登録済みデータと一致するかを判定し、一致した場合は、ユーザデバイスＩＤに基づくマスターパスワードの検索あるいはマスターキーを用いたマスターパスワードの生成処理を実行する。サポートセンタは、情報処理装置と

してのユーザデバイスに対応して設定されたデバイス識別子としてのデバイスＩＤと、マスターパスワードとを対応させたマスターパスワード格納データベースを有する。あるいは、デバイスＩＤと、デバイス個々に固有のキー、または一群のデバイスに共通するキーとして設定されたマスターキーとを対応させたマスターキー格納データベースのいずれかを有し、マスターパスワード格納データベースを有する場合には、デバイスＩＤに基づいてデータベース検索を実行してマスターパスワードを取得する。マスターキー格納データベースを有する場合には、デバイスＩＤに対する、マスターキーを適用した暗号処理によるマスターパスワード生成処理を実行し、生成したマスターパスワードをユーザデバイスに送付する処理を実行する。

【０１３３】ユーザデバイスＩＤに基づくマスターキーによるマスターパスワードの生成処理フローを図１４に示す。図１４のフローについて説明する。まず、ステップＳ１０１において、マスターキーＫｍ１を用いてデバイスＩＤの暗号化処理を実行する。その結果をステップＳ１０２において、ＭＰａとする。さらに、結果ＭＰａに対してマスタキーＫｍ２を適用した暗号化処理を実行してパスワードＭＰを得て、ステップＳ１０３において、ＡＳＣＩＩコードに変換する。暗号化処理は例えばＤＥＳ，トリプルＤＥＳ等の暗号化アルゴリズムが適用可能である。マスターキーＫｍ１，Ｋｍ２は、複数のデバイスに対して共通に設定されたキーであり、サポートセンタはユーザデバイスＩＤに基づいて、サポートセンタで保持する複数のキーから適用すべきマスターキーを選択して使用する。

【０１３４】図１３のシーケンス図に戻って説明を続ける。サポートセンタでマスターパスワードの生成が実行されると、サポートセンタは、マスターパスワードをオンラインまたはオフラインでユーザまたはユーザデバイスに対して送信または送付する。

【０１３５】以上のシーケンスに従って、ユーザは、サポートセンタを利用してマスターパスワードの再発行処理を行なうことができる。なお、ユーザデバイスと、サポートセンタ間においては、データ送受信の前処理として相互認証処理を実行し、送受信する秘密データ、例えばユーザＩＤ、マスターパスワード等は相互認証時に生成したセッションキーで暗号化し、またデータの改竄防止のために署名の生成、検証を行なうことが好ましい。なお、これら相互認証処理、署名生成、検証処理等の詳細については、コンテンツの配信処理の項目で詳しく説明する。

【０１３６】また、ユーザは、サポートセンタを利用したマスターパスワードの再発行処理をオフラインで行なうことも可能である。この場合は、ハガキなどに本人確認のための情報を記入して送付するなどの処理が行なわれることになる。

【０１３７】［コンテンツ配信処理］ユーザデバイス内のセキュリティチップ内のメモリ領域にサービスプロバイダの管理領域が登録され、サービスプロバイダとの認証に必要な情報、上記パスワード等が登録されると、これらの情報を用いてサービスプロバイダとの通信によるコンテンツ購入が可能となる。以下、コンテンツ購入処理の詳細について説明する。

【０１３８】コンテンツ購入処理における概要を説明するシーケンス図を図１５に示す。左側がセキュリティチップを持つユーザデバイス側処理であり、右側がサービスプロバイダ側処理である。

【０１３９】ユーザデバイスは、まず、コンテンツの購入要求をサービスプロバイダに出力する。サービスプロバイダがコンテンツ購入要求を受信すると、ユーザデバイスとサービスプロバイダ間において相互認証が実行される。相互認証が成立し、双方の正当性が確認されると、サービスプロバイダは、購入要求コンテンツに対応する属性証明書（ＡＣ:Attribute Certificate）を生成し、ユーザデバイスに送信する。属性証明書には、コンテンツを復号するためのコンテンツ鍵：Ｋｃが暗号化されて格納され、また、利用回数、利用期限等のコンテンツ利用条件が記録されている。また格納データに対して属性証明書発行者である属性証明書認証局（ＡＡ:Attribute Certificate Authority）の署名がなされており、改竄防止を考慮したものとなっている。

【０１４０】属性証明書を受信したユーザデバイスは、属性証明書の署名検証処理を実行し、改竄なしの判定に基づいて属性証明書をメモリに保存する。さらに、ユーザデバイスは、コンテンツの要求をサービスプロバイダに対して行ない、サービスプロバイダは、先にユーザデバイスに送付した属性証明書内に格納されたコンテンツ鍵：Ｋｃで暗号化したコンテンツをユーザデバイスに送付する。ユーザデバイス側では、属性証明書から取り出した暗号化されたコンテンツ鍵の復号化処理を実行してコンテンツ鍵を取り出し、取り出したコンテンツ鍵を適用した暗号化コンテンツの復号化処理によりコンテンツを取得し、利用する。なお、属性証明書に格納したコンテンツ鍵の復号化処理をサービスプロバイダ側で実行する態様（オンライン復号）もある。これらの具体的処理例については、後段で説明する。

【０１４１】コンテンツ配信に伴う大まかな流れは、以上、図１５を用いて説明した通りである。以下、各処理の詳細について説明する。なお、図１５に示した処理シーケンスでは、コンテンツに対応する属性証明書を暗号化コンテンツ送付の先に実行しているが、暗号化コンテンツの配信と、属性証明書の配信はいずれが先でもよく、同時に配信する処理としてもよい。また、それぞれをディスク等の記録媒体に格納して配信するオフライン配信を行なう構成とすることも可能である。

【０１４２】また、サービスプロバイダからユーザデバ

イスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０１４３】（１）相互認証処理、

コンテンツの購入要求エンティテイであるユーザデバイス、およびコンテンツの提供元であるサービスプロバイダ間では、まず相互認証処理が実行される。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

【０１４４】ここでは、公開鍵暗号方式の１つの認証処理方式であるハンドシェイクプロトコル（ＴＬＳ１．０）について図１６のシーケンス図を参照して説明する。

【０１４５】図１６において、左側がユーザデバイス(クライアント)の処理、右側がサービスプロバイダ（サーバ）側の処理を示している。まず、（１）サービスプロバイダ（サーバ）が暗号化仕様を決定するためのネゴシエーション開始要求をハローリクエストとしてユーザデバイス（クライアント）に送信する。（２）ユーザデバイス（クライアント）はハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションＩＤ、プロトコルバージョンの候補をクライアントハローとして、サービスプロバイダ（サーバ）側に送信する。

【０１４６】（３）サービスプロバイダ（サーバ）側は、利用を決定した暗号化アルゴリズム、セッションI.D、プロトコルバージョンをサーバーハローとしてユーザデバイス（クライアント）に送信する。（４）サービスプロバイダ（サーバ）は、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をユーザデバイス（クライアント）に送信（サーバ・サーティフィケート）する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式を送付する必要はない。（５）サービスプロバイダ（サーバ）は、ＲＳＡ公開鍵またはＤｉｆｆｉｅ＆Ｈｅｌｌｍａｎ公開鍵情報をユーザデバイス（クライアント）に送信（サーバ・キー・エクスチェンジ）する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

【０１４７】（６）次にサービスプロバイダ（サーバ）側は、ユーザデバイス（クライアント）に対してサーティフィケート・リクエストとして、ユーザデバイス（クライアント）の有する証明書を要求し、（７）サービスプロバイダ（サーバ）によるネゴシエーション処理の終了を知らせる（サーバハロー終了）。

【０１４８】（８）サーバハロー終了を受信したユーザデバイス（クライアント）は、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をサービスプロバイダ（サーバ）に送信（クライアント・サーティフィケート）する。なお、公開鍵証明書の連鎖検証を行なわない場合は公開鍵証明書の一式送付は必須ではない。（９）ユーザデバイス（クライアント）は、４８バイト乱数をサービスプロバイダ（サーバ）の公開鍵で暗号化してサービスプロバイダ（サーバ）に送信する。サービスプロバイダ（サーバ）、ユーザデバイス（クライアント）は、この値をもとに送受信データ検証処理のためのメッセージ認証コード：ＭＡＣ（Message Authentication Code）生成用のデータ等を含むマスターシークレットを生成する。

【０１４９】（１０）ユーザデバイス（クライアント）は、クライアント証明書の正しさを確認するため、ここまでのメッセージのダイジェストをクライアントの秘密鍵で暗号化してサービスプロバイダ（サーバ）に送信（クライアントサーティフィケート確認）し、（１１）先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１２）認証の終了を通知する。一方、（１３）サービスプロバイダ（サーバ）側からユーザデバイス（クライアント）に対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１４）認証の終了を通知する。

【０１５０】上記処理において決定された暗号化アルゴリズムに従ってユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間のデータ転送が実行されることになる。

【０１５１】データ改竄の検証は、上述の認証処理でユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：ＭＡＣ（Message Authentication Code）を各エンティテイの送信データに付加することでメッセージの改竄検証を行なう。

【０１５２】図１７にメッセージ認証コード：ＭＡＣ（Message Authentication Code）の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成される

ＭＡＣシークレットを付加し、これらの全体データからハッシュ値を計算し、さらにＭＡＣシークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード（ＭＡＣ）を生成する。この生成したＭＡＣを送信データに付加して、受信側で受信データに基づいて生成したＭＡＣと受信ＭＡＣとの一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

【０１５３】（２）コンテンツ利用権限情報証明書（属性証明書）の生成、送信

ユーザデバイスからコンテンツの要求がなされたサービスプロバイダは、要求コンテンツの復号化処理に適用可能なコンテンツ鍵：Ｋｃを暗号化して格納し、コンテンツの利用制限情報を格納したコンテンツ利用権限情報証明書、例えば属性証明書（ＡＣ）を生成して、ユーザに対して送信する。

【０１５４】コンテンツ利用権限情報証明書、例えば属性証明書（ＡＣ）を生成する主体は、サービスプロバイダ自身であっても、またコンテンツ管理を実行する外部エンティティであってもよい。外部エンティティが属性証明書（ＡＣ）を生成する場合は、サービスプロバイダの要求に従ってその外部エンティティが属性証明書（ＡＣ）を生成する。

【０１５５】属性証明書には対応暗号化コンテンツの復号に適用可能なコンテンツ鍵：Ｋｃが暗号化されて格納される。コンテンツ鍵Ｋｃの暗号化に適用する鍵には、例えば、

（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ

（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋ

（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇ

の各態様がある。なお、この他にも、いくつかの態様が可能である。例えばサービスプロバイダの保有する公開鍵で暗号化することも可能である。この場合は、ユーザデバイスから属性証明書（ＡＣ）を受信してサービスプロバイダの保有する秘密鍵で復号化することになる。

【０１５６】なお、いずれの暗号化態様を適用した場合でも、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。以下、上記（ａ）～（ｃ）の態様における処理の詳細について説明する。

【０１５７】（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを適用した場合

前述したユーザデバイスのセキュリティチップのメモリ領域についての説明中で示したように、ユーザデバイスに登録された各登録サービスプロバイダについては、メモリに形成された各サービスプロバイダ管理領域にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋが格納される。ユーザデバイスのセキュリティチップでは、サービスプロバイダから提供されるコンテンツに対応する属性証明書の中からＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋで暗号化されたコンテンツ鍵：Ｋｃ、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、ＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋで復号化処理を実行することにより、コンテンツ鍵：Ｋｃを取得する。なお、［Ａ（Ｂ）］は、Ａで暗号化されたＢからなるデータを示すものとする。本形態では、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することなくユーザデバイス内の処理としてコンテンツ復号、すなわちオフライン復号が可能となる。

【０１５８】なお、上記例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成例について説明したが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納する。

【０１５９】（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋを適用した場合

サービスプロバイダは、ユーザデバイスに対して提供するコンテンツに対応して設定される属性証明書に格納するコンテンツ鍵：Ｋｃをサービスプロバイダが保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを適用して暗号化する。ユーザデバイスは、属性証明書を受信しても、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］を復号することはできない。サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋはユーザデバイスは保有していないからである。

【０１６０】従って、コンテンツを利用（復号化）する

ためには、次のような処理が必要となる。まず、ユーザデバイスは、サービスプロバイダに属性証明書を送付してコンテンツ鍵の復号要求を行ない、サービスプロバイダにおいては、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋによってコンテンツ鍵：Ｋｃの復号化を行なう。ユーザデバイスはサービスプロバイダより復号化されたコンテンツ鍵：Ｋｃを取得し、該コンテンツ鍵：Ｋｃで暗号化コンテンツの復号を行なう。本形態では、上述の（ａ）の形態と異なり、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することが必須となる。すなわちオンライン処理が必要となる。

【０１６１】（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを適用した場合

このグローバル共通鍵を利用する形態は、コンテンツの配信を実行するサービスプロバイダにおいて、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ（ＳＨ）による管理されたコンテンツ配信を行なうための構成である。サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇの各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納し、コンテンツ利用者としてのエンドエンティティであるユーザデバイスに配布することで、サービスプロバイダ自体もコンテンツ鍵を取り出すことを防止し、ユーザデバイスにおいてのみコンテンツ鍵：Ｋｃを取り出すことを可能とした構成である。

【０１６２】以下、これらの各形態について詳細に説明する。まず、上記（ａ）～（ｃ）に共通する属性証明書の発行処理シーケンスについて図１８を用いて説明する。

【０１６３】図１８の処理シーケンスは、先に説明した図１５のコンテンツ購入処理シーケンスの一部として構成される属性証明書の生成、送信処理を詳細に説明したものである。ユーザデバイスはセキュリティチップを内蔵し、セキュリティチップ内のメモリにはサービスプロバイダ管理領域が生成されており、サービスプロバイダ管理情報が格納済みであるとする。

【０１６４】図１８の処理について説明する。ユーザデバイスとサービスプロバイダ間の相互認証が成立後、

（１）セキュリティチップを持つユーザデバイスは、サービスプロバイダに対して属性証明書（ＡＣ）の要求を行なう。属性証明書（ＡＣ）要求には、サービスプロバイダ管理領域に登録されたユーザＩＤ、コンテンツの指定識別子としてのアプリケーションＩＤ、さらにユーザが選択した利用条件データにユーザの秘密鍵（サービスプロバイダ対応秘密鍵）で署名したデータにユーザの公開鍵証明書（ＰＫＣ）を添付して送信する。利用条件データは、例えばコンテンツ利用制限回数、利用期限等の指定データであり、ユーザによって選択可能である場合にユーザ指定データとして含まれる。

【０１６５】署名は、データ改竄の検証を可能とするために付加されるものであり、前述のＭＡＣ値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

【０１６６】公開鍵暗号方式を用いた電子署名の生成方法について、図１９を用いて説明する。図１９に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital SignatureAlgorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptosystem（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【０１６７】図１９の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$，$4a^3+27b^2\neq 0$（ｍｏｄ　ｐ））、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【０１６８】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【０１６９】続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【０１７０】

【数１】Ｐ=(Ｘａ，Ｙａ),Ｑ=(Ｘｂ，Ｙｂ),Ｒ=(Ｘｃ,Ｙｃ)=Ｐ+Ｑとすると、

Ｐ≠Ｑの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$
P=Qの時（2倍算）、
$Xc=\lambda^2-2Xa$
$Yc=\lambda\times(Xa-Xc)-Ya$
$\lambda=(3(Xa)^2+a)/(2Ya)$

【０１７１】これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、ｕを2進数展開して1が立っているところに対応する$2^i\times G$（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【０１７２】ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【０１７３】ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１７４】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図２０を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$，$4a^3+27b^2\neq0$（ｍｏｄ　ｐ））、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２=ｃｈｍｏｄ　ｒを計算する。

【０１７５】ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、ベースポイントＧおよびＫｓ×Ｇを知っているので、図１９のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ　ｍｏｄ　ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１７６】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１７７】ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ　ｍｏｄ　ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１７８】ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

【０１７９】属性証明書（ＡＣ）要求を受信したサービスプロバイダは、上述の署名検証処理等によって要求データに改竄がないことを確認すると、アプリケーションＩＤで特定されるコンテンツに対応するコンテンツ鍵：Ｋｃを暗号化する。このコンテンツ鍵：Ｋｃの暗号化に適用する鍵は、前述の（ａ）ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋ、（ｂ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋ、（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇのいずれかである。

【０１８０】さらに、サービスプロバイダは、コンテンツの利用条件データ他の必要データを格納し、前述した図５に示す属性証明書を生成する。生成した属性証明書には、サービスプロバイダの秘密鍵を用いた電子署名が付加される。電子署名の生成処理は、図１９の処理フローと同様の処理に従って実行される。サービスプロバイダによって生成された属性証明書はユーザデバイスに送付され、ユーザデバイスにおいて、上述の図２０の処理フローと同様のシーケンスに従って署名検証処理を実行する。

【０１８１】さらに、必要に応じてユーザデバイスは、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０１８２】属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）との関連確認処理、および各証明書の検証処理の詳細について、図を参照して説明する。図２１のフローは、属性証明書（ＡＣ）の検証を実行する際に行なわれる属性証明書（ＡＣ）に関連する公開鍵証明書（ＰＫＣ）の確認処理である。

【０１８３】確認対象の属性証明書（ＡＣ）がセット（Ｓ２１）されると、属性証明書のＡＣ保持者の公開鍵証明書情報（ｈｏｌｄｅｒ）フィールドを抽出（Ｓ２２）し、抽出した公開鍵証明書情報（ｈｏｌｄｅｒ）フィールド内に格納された公開鍵証明書の発行者情報（ＰＫＣ　ｉｓｓｕｅｒ）、公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）を確認（Ｓ２３）し、公開鍵証明書の発行者情報（ＰＫＣｉｓｓｕｅｒ）、公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）に基づいて公開鍵証明書（ＰＫＣ）を検索（Ｓ２４）して、属性証明書（ＡＣ）に関連付けられた公開鍵証明書（ＰＫＣ）を取得（Ｓ２５）する。

【０１８４】図２１に示すように、属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）とは、属性証明書に格納された公開鍵証明書情報（ｈｏｌｄｅｒ）フィールド内の公開鍵証明書発行者情報（ＰＫＣ　ｉｓｓｕｅｒ）、および公開鍵証明書シリアル番号（ＰＫＣ　ｓｅｒｉａｌ）により関連付けがなされている。

【０１８５】次に、図２２を参照して公開鍵証明書（ＰＫＣ）の検証処理について説明する。図２２に示す公開鍵証明書（ＰＫＣ）の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書（ＰＫＣ）をセット（Ｓ３１）し、公開鍵証明書（ＰＫＣ）格納情報に基づいて、公開鍵証明書（ＰＫＣ）署名者を特定（Ｓ３２）する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定（Ｓ３３）し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ３４）する。最上位公開鍵証明書が取得されセット（Ｓ３５）されると、署名検証に必要な検証鍵（公開鍵）を取得（Ｓ３６）し、検証対象の署名が自己署名であるか否かを判定し（Ｓ３７）、自己署名でない場合は、下位ＰＫＣをセット（Ｓ３９）して、上位の公開鍵証明書から取得した検証鍵（公開鍵）に基づいて署名検証を実行（Ｓ４０）する。なお、ステップＳ３７における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行（Ｓ３８）し、ステップＳ４１に進む。

【０１８６】署名検証に成功した場合（Ｓ４１：Ｙｅｓ）は、目的とするＰＫＣの検証が完了したか否かを判定（Ｓ４２）し、完了している場合は、ＰＫＣ検証を終了する。完了していない場合は、ステップＳ３６に戻り、署名検証に必要な検証鍵（公開鍵）の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合（Ｓ４１：Ｎｏ）は、ステップＳ４３に進み、エラー処理、例えばその後の手続きを停止する等の処理を実行する。

【０１８７】次に、図２３を参照して属性証明書（ＡＣ）の検証処理（例１）について説明する。まず、検証対象となる属性証明書（ＡＣ）をセット（Ｓ５１）し、属性証明書（ＡＣ）格納情報に基づいて、属性証明書（ＡＣ）の所有者および署名者を特定（Ｓ５２）する。さらに、属性証明書（ＡＣ）の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５３）して、公開鍵証明書の検証処理を実行（Ｓ５４）する。

【０１８８】公開鍵証明書の検証に失敗した場合（Ｓ５５でＮｏ）は、ステップＳ５６に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５５でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５７）して、公開鍵証明書の検証処理を実行（Ｓ５８）する。公開鍵証明書の検証に失敗した場合（Ｓ５９でＮｏ）は、ステップＳ６０に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５９でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書から公開鍵を取り出し（Ｓ６１）て、取り出した公開鍵を用いて属性証明書（ＡＣ）の署名検証処理を実行（Ｓ６２）する。署名検証に失敗した場合（Ｓ６３でＮｏ）は、ステップＳ６４に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ６３でＹｅｓ）は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテンツ鍵の取得等に移行する。

【０１８９】次に、図２４を参照して属性証明書（ＡＣ）の検証処理（例２）について説明する。本例は、自デバイス内に属性証明書（ＡＣ）の検証処理に必要となる公開鍵証明書が格納されているか否かを判定し、公開鍵証明書が格納されている場合は、その検証を省略することとした例である。まず、検証対象となる属性証明書（ＡＣ）をセット（Ｓ７１）し、属性証明書（ＡＣ）格納情報に基づいて、属性証明書（ＡＣ）の所有者および署名者を特定（Ｓ７２）する。さらに、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに格納保存されていないかを検索（Ｓ７３）する。保存されている場合（Ｓ７４でＹｅｓ）は、属性証明書（ＡＣ）の所有者の公開鍵証明書を取り出し（Ｓ７５）て、ステップＳ８１に進む。

【０１９０】属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに保存されていない場合（Ｓ７４でＮｏ）は、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）を直接あるいはリポジトリ

などから取得（Ｓ７６）して、属性証明書（ＡＣ）の所有者の公開鍵証明書（ＰＫＣ）の検証処理を実行（Ｓ７７）する。公開鍵証明書の検証に失敗した場合（Ｓ７８でＮｏ）は、ステップＳ７９に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ７８でＹｅｓ）は、公開鍵証明書の検証結果を保存（Ｓ８０）した後、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに格納保存されていないかを検索（Ｓ８１）する。保存されている場合（Ｓ８２でＹｅｓ）は、属性証明書（ＡＣ）の署名者の公開鍵証明書を取り出し（Ｓ８３）て、ステップＳ８８に進む。

【０１９１】属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）が自デバイス内のメモリに保存されていない場合（Ｓ８２でＮｏ）は、属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）を直接あるいはリポジトリなどから取得（Ｓ８４）して、属性証明書（ＡＣ）の署名者の公開鍵証明書（ＰＫＣ）の検証処理を実行（Ｓ８５）する。公開鍵証明書の検証に失敗した場合（Ｓ８６でＮｏ）は、ステップＳ８７に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ８６でＹｅｓ）は、公開鍵証明書から属性証明書（ＡＣ）の署名検証に適用する鍵（公開鍵）を取り出し（Ｓ８８）、属性証明書（ＡＣ）の署名検証処理を実行（Ｓ８９）する。署名検証に失敗した場合（Ｓ９０でＮｏ）は、ステップＳ９１に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ９０でＹｅｓ）は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテンツ鍵の取得等に移行する。

【０１９２】ユーザデバイスによる属性証明書の検証がなされると、属性証明書はユーザデバイス内のセキュリティチップのメモリ、あるいはセキュリティチップ外のユーザデバイス制御部の管理下の外部メモリに格納され、コンテンツの利用時に、属性証明書内の暗号化コンテンツ鍵の取得、復号化処理を実行することになる。属性証明書から暗号化されたコンテンツ鍵を取得して復号する処理について、以下説明する。

【０１９３】（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを適用した場合

まず、前述の（ａ）ＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋをコンテンツ鍵：Ｋｃの暗号化に適用し、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【０１９４】ＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋは、サービスプロバイダ管理領域に格納され、ユーザは前述した認証情報（パスワード）入力により、この鍵を取り出して利用することができる。従って、コンテンツ鍵：Ｋｃはサービスプロバイダに接続することなくオフライン処理として取得可能であり、コンテンツの復号が可能となる。

【０１９５】図２５に属性証明書からの暗号化コンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【０１９６】図２５のシーケンス図に従って説明する。図２５は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部の処理を示している。まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションＩＤをセキュリティチップ制御部に送信し、メモリからアプリケーションＩＤに対応する属性証明書（ＡＣ）を取得する。ユーザデバイスでは、アプリケーションＩＤに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Ｋｃの取得（復号）処理を要求する。

【０１９７】セキュリティチップ制御部は、属性証明書の署名検証を実行し、データ改竄のないことを確認し、属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０１９８】次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツを、セキュリティチップ制御部を介してメモリから取得する。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

【０１９９】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、暗号化コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプ

ロバイダ管理領域に格納される。

【０２００】（ｂ）サービスプロバイダの保有する秘密鍵（共通鍵系）：ＳＰ．Ｓｔｏ．Ｋを適用した場合

次に、前述の（ｂ）サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋをコンテンツ鍵：Ｋｃの暗号化に適用し、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【０２０１】サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋは、サービスプロバイダが保有し、ユーザデバイスには格納されていない鍵である。従って、ユーザデバイスがコンテンツ鍵：Ｋｃを取得するためには、サービスプロバイダに接続して、コンテンツ鍵の復号化処理をサービスプロバイダに対して要求することが必要となり、オンライン処理によるコンテンツ復号を実行することとなる。

【０２０２】図２６に属性証明書からのコンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【０２０３】図２６のシーケンス図に従って説明する。図２６は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダにおける処理を示している。

【０２０４】まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションＩＤをセキュリティチップ制御部に送信し、メモリからアプリケーションＩＤに対応する属性証明書（ＡＣ）を取得する。ユーザデバイスでは、アプリケーションＩＤに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Ｋｃの取得（復号）処理を要求する。

【０２０５】セキュリティチップ制御部は、属性証明書の検証の後、属性証明書の発行元であるサービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０２０６】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０２０７】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。さらに、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０２０８】セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。

【０２０９】コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツをセキュリティチップ制御部を介してメモリから取得する。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

【０２１０】（ｃ）システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを適用した場合

次に、システムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Ｋｇを、コンテンツ鍵：Ｋｃの暗号化に間接的に適用して属性証明書に格納する処理形態について説明する。このグローバル共通鍵を利用する形態は、ユーザデバイスにおいてのみコンテンツ鍵：Ｋｃを取り出すことを可能とし、コンテンツの配信を実行するサービスプロバイダはコンテンツ鍵の取り出しを不可能とすることで、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ（ＳＨ）による管理されたコンテンツ配信を行なうことが可能となる。

【０２１１】具体的には、サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ（ＳＨ）とユーザデバイスで共有する鍵として生

成されるグローバル共通鍵：Ｋｇの各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納する。

【０２１２】図２７に、グローバル共通鍵：Ｋｇをコンテンツ鍵：Ｋｃの暗号化に間接的に適用してコンテンツ鍵：Ｋｃの暗号化データを属性証明書に格納して配布する処理の詳細を説明する図を示す。

【０２１３】図２７には、コンテンツ配信のプラットホームを構築、管理するシステムホルダ３０１、コンテンツ配信を実行するサービスプロバイダ（ＣＤ：コンテンツディストリビュータ）３０２、コンテンツを生成または管理し、サービスプロバイダ３０２に対して暗号化コンテンツを提供するコンテンツクリエータ３０３、サービスプロバイダ３０２からコンテンツを受領するエンドエンティティとしてのユーザデバイス３０４を示している。なお、ユーザデバイス３０４は、前述の（ａ），（ｂ）の例と同様、セキュリティチップを有し、セキュリティチップ内のメモリ領域にはサービスプロバイダ管理領域が生成されている。

【０２１４】図２７の処理について説明する。まず、コンテンツクリエータ３０３は、配信対象となるコンテンツを暗号化するための鍵：Ｋｃを例えば乱数により生成し、生成したコンテンツ鍵（共通鍵系）：Ｋｃを用いて、（１）コンテンツを暗号化してサービスプロバイダ３０２に提供する。

【０２１５】さらに、システムホルダ３０１は、（２）コンテンツクリエータ３０３から、コンテンツクリエータ３０３の保有するコンテンツクリエータ鍵（共通鍵系）：Ｋｃｃを受信し、（３）サービスプロバイダ（ＣＤ：コンテンツディストリビュータ）３０２からサービスプロバイダ３０２の保有するサービスプロバイダ鍵（共通鍵系）：Ｋｃｄを受信する。なお、これらの鍵は事前に受け渡しを行なってもよい。

【０２１６】システムホルダ３０１は、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化する。すなわち暗号化鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］を生成し、（４）これをコンテンツクリエータ３０３に送付する。なお、［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］は事前に受け渡しを行なってもよい。グローバル共通鍵：Ｋｇは、システムホルダ３０１と、ユーザデバイス３０４が共有する鍵である。ユーザデバイス３０４には、（５）デバイス製造時、デバイス販売時まで、あるいは少なくともコンテンツの購入開始前までに、１以上のグローバル共通鍵：Ｋｇ１～Ｋｇｎが格納され、これらはシステムホルダの管理の下に更新処理が実行される。更新処理については、後述する。

【０２１７】コンテンツクリエータ３０３は、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］を生成し、（６）これをサービスプロバイダ３０２に対して送信するとともに、システムホルダ３０１から受信した、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化した暗号化鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］をサービスプロバイダ３０２に対して送信する。なお、［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］は事前に受け渡しを行なってもよい。

【０２１８】ユーザデバイス３０４がサービスプロバイダ３０２に対して（７）コンテンツ購入要求を行なうと、（８）サービスプロバイダは、要求コンテンツに対応する属性証明書を生成して、ユーザデバイス３０４に送信する。生成する属性証明書（ＡＣ）には、前述の暗号鍵データ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］、すなわち、コンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ、および、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］が格納される。その他、コンテンツの利用条件等のデータが格納され、サービスプロバイダ３０２の電子署名がなされてユーザデバイス３０４に送信される。ユーザデバイス３０４は、受信した属性証明書（ＡＣ）をメモリに格納する。

【０２１９】コンテンツの利用時には、ユーザデバイス３０４は、サービスプロバイダ３０２との間で（９）相互認証を行なった後、（１０）先に受信済みの属性証明書（ＡＣ）をサービスプロバイダ３０２に送信する。相互認証処理は、ユーザデバイスのセキュリティチップとサービスプロバイダ間の相互認証処理として実行される。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０２２０】属性証明書には、前述のコンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］、および、コンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］が格納されている。

【０２２１】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検

証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（１１）サービスプロバイダは、自己の所有するサービスプロバイダ鍵：Ｋｃｄを、相互認証時に生成したセッション鍵：Ｋｓｅｓで暗号化して、暗号化鍵データ［Ｋｓｅｓ（Ｋｃｄ）］を生成し、これをユーザデバイスに送信する。

【０２２２】ユーザデバイス３０４のセキュリティチップ制御部は、（１２）サービスプロバイダ３０２から受信した暗号化鍵データ［Ｋｓｅｓ（Ｋｃｄ）］について、セッションキーを用いた復号化処理を実行してサービスプロバイダ鍵：Ｋｃｄを取得する。なお、サービスプロバイダ鍵：Ｋｃｄを事前にサービスプロバイダメモリ領域に保管しておいてもよい。

【０２２３】ユーザデバイス３０４のセキュリティチップ制御部は、次に、（１３）属性証明書中のコンテンツクリエータ鍵：Ｋｃｃをサービスプロバイダ鍵：Ｋｃｄで暗号化し、さらに、この暗号化データをグローバル共通鍵：Ｋｇで暗号化したデータ：［Ｋｇ（［Ｋｃｄ（Ｋｃｃ）］）］について、まず、自己の所有するグローバル共通鍵：Ｋｇで復号し、［Ｋｃｄ（Ｋｃｃ）］を取得する。さらに、（１４）サービスプロバイダ３０２から受信した暗号化鍵データの復号により取得したサービスプロバイダ鍵：Ｋｃｄを適用した復号化処理により、コンテンツクリエータ鍵：Ｋｃｃを取得する。

【０２２４】さらに、（１５）ユーザデバイス３０４のセキュリティチップ制御部は、属性証明書中のコンテンツ鍵：Ｋｃをコンテンツクリエータ鍵：Ｋｃｃで暗号化したデータ：［Ｋｃｃ（Ｋｃ）］を取り出して、前記処理によって取得したコンテンツクリエータ鍵：Ｋｃｃを適用した復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。

【０２２５】コンテンツ鍵：Ｋｃの取得に成功すると、ユーザデバイス３０４のセキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２２６】ユーザデバイス３０４は、サービスプロバイダ３０２から取得した暗号化コンテンツ（（１６）の処理）をセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行する。

【０２２７】なお、上述の各エンティティ間における鍵、暗号化鍵等のデータ送受信の前には、データ送受信を実行するエンティティ間で相互認証を実行し、認証成立を条件としたデータ送受信を行なうことが好ましく、また送受信データはセッションキーで暗号化し、署名を付与した構成とすることが好ましい。

【０２２８】このように、グローバル共通鍵は、ユーザデバイスとシステムホルダのみが所有し、その他のエンティティは保有することがなく、他のエンティティでは取得不可能な鍵として構成される。従って、サービスプロバイダにおいてもコンテンツ鍵の取得は不可能であり、システムホルダの許可のないコンテンツ鍵の流通、コンテンツの流通が防止可能となる。

【０２２９】グローバル共通鍵は、必要に応じて更新される。更新を実行するのは、システムホルダの管理下にあるサポートセンタである。サポートセンタとユーザデバイス間で実行されるグローバル共通鍵更新処理シーケンスを図２８に示す。ユーザデバイスのセキュリティチップ内のメモリ領域には、２つのグローバル共通鍵Ｋｇ１，Ｋｇ２が格納されているものとする。これらのいずれかを使用して属性証明書内の鍵データの暗号化がなされ、復号化処理が実行される。あるいは例えばトリプルＤＥＳアルゴリズムを適用して２つの鍵を用いて属性証明書内の鍵データの暗号化を行ない、２つの鍵を用いた復号化処理を実行する構成としてもよい。

【０２３０】図２８の処理シーケンスに示す各処理について説明する。図２８は左からセキュリティチップ制御部、ユーザデバイス制御部、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【０２３１】まず、ユーザデバイス制御部がグローバル共通鍵：Ｋｇ更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、システムホルダの管理下にあるサポートセンタに対してユーザデバイスを介して接続し、セキュリティチップとサポートセンタ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。

【０２３２】相互認証が成立すると、セキュリティチップの制御部は、サポートセンタに対してグローバル共通鍵：Ｋｇ更新要求を出力する。サポートセンタは、すでに生成済みの更新用グローバル共通鍵：Ｋｇ３、あるいは要求に応じて生成したグローバル共通鍵：Ｋｇ３を認証処理において生成したセッション鍵：Ｋｓｅｓで暗号化し、暗号化鍵データ：［Ｋｓｅｓ（Ｋｇ３）］をユーザデバイスのセキュリティチップに対して送信する。

【０２３３】セキュリティチップの制御部は、サポートセンタからセッションキーで暗号化されたグローバル共通鍵：Ｋｇ３、すなわち、［Ｋｓｅｓ（Ｋｇ３）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してグローバル共通鍵：Ｋｇ３を取得する。

【０２３４】グローバル共通鍵：Ｋｇ３の取得に成功すると、セキュリティチップ制御部は、グローバル共通鍵：Ｋｇ１を、取得したグローバル共通鍵：Ｋｇ３に置

き換える。これにより、ユーザデバイスの保有するグローバル共通鍵は、Ｋｇ２、Ｋｇ３となる。ユーザデバイスの保有するグローバル共通鍵は、その順序関係も含めて意味があるため、［Ｋｇ１，Ｋｇ２］の順序関係も併せて［Ｋｇ２，Ｋｇ３］と修正する。グローバル共通鍵は、鍵データと共にユーザデバイス内で保持されている順序関係も合わせてデータを保持しているものとする。

【０２３５】図２９は、ユーザデバイスとサポートセンタが直接データ送受信を行なうことなく、サービスプロバイダが仲介を行なってグローバル共通鍵の更新を実行する処理シーケンス例を示した図である。

【０２３６】図２９の処理シーケンスに示す各処理について説明する。図２９は左からセキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダ、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【０２３７】サポートセンタでは、更新される新たなグローバル共通鍵：Ｋｇ３を事前生成し、グローバル共通鍵：Ｋｇ３をすでにユーザデバイスに配布済みのグローバル共通鍵：Ｋｇ２で暗号化してデータ：［Ｋｇ２（Ｋｇ３）］を生成し、これに、サポートセンタの秘密鍵：Ｋｓｓで署名を付してサービスプロバイダに送付する。サービスプロバイダは、データ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［Ｋｓｓ］を有する。なお、Ａ，Ｓｉｇ［Ｂ］は、データＡに鍵Ｂで署名を付加したデータ構成を示すものとする。

【０２３８】次に、ユーザデバイス制御部がグローバル共通鍵：Ｋｇ更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、サービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。

【０２３９】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対してグローバル共通鍵：Ｋｇ更新要求を出力する。サービスプロバイダはサポートセンタから受信済みのデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］をユーザデバイスのセキュリティチップに対して送信する。

【０２４０】セキュリティチップの制御部は、サービスプロバイダから、サポートセンタからのデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］の転送を受けると、署名検証処理を実行し、データ改竄のないことを確認した後、自己の所有するグローバル共通鍵：Ｋｇ２で暗号化されたグローバル共通鍵：Ｋｇ３、すなわち、［Ｋｇ２（Ｋｇ３）］に対して、グローバル共通鍵：Ｋｇ２を用いた復号化処理を実行してグローバル共通鍵：Ｋｇ３を取得する。なお、サポートセンタの署名検証にサポートセンタの公開鍵を適用する場合は、サポートセンタの公開鍵証明書をユーザデバイスに対してデータ［Ｋｇ２（Ｋｇ３）］，Ｓｉｇ［ＳｕＣ］とともに送信するか、あるいはユーザデバイスに予め配布しておく。

【０２４１】グローバル共通鍵：Ｋｇ３の取得に成功すると、セキュリティチップ制御部は、メモリの鍵格納領域、例えば前述のデバイス管理領域内のグローバル共通鍵：Ｋｇ１書き込み領域にグローバル共通鍵：Ｋｇ３を上書きする。この更新処理により、ユーザデバイスの保有するグローバル共通鍵は、Ｋｇ２、Ｋｇ３の２つに更新される。

【０２４２】［デコーダを利用した復号化処理］暗号化コンテンツ、あるいは暗号化コンテンツ鍵は、専用の復号化処理機能を持つデコーダに処理を実行させる構成とすると処理の高速化が可能となる。ただし、デコーダはセキュリティチップと独立したハード構成を持つため、デコーダの信頼性を確認した上でデコーダ内でのコンテンツ鍵、コンテンツの復号化を行なうことが必要となる。以下、デコーダを用いた暗号化コンテンツ、あるいは暗号化コンテンツ鍵の復号化処理について図を参照して説明する。

【０２４３】図３０にユーザデバイスにセキュリティチップと、デコーダを有する場合のコンテンツ鍵、コンテンツの復号化処理シーケンスを説明する図を示す。

【０２４４】ユーザデバイスは、セキュリティチップ２１０と、デコーダ２８０、ハードディスク、フラッシュメモリ等からなるメモリ部２２２と、上位ソフトウェアによりセキュリティチップ２１０と、デコーダ２８０、メモリ部２２２に対してデータ入出力、各種処理実行命令を行なうユーザデバイス側制御部２２１がある。

【０２４５】コンテンツ復号化処理時のシーケンスについて説明する。まず、ユーザによる入力手段の操作により、コンテンツを指定したコンテンツ利用要求がユーザデバイス側制御部２２１に入力されると、ユーザデバイス側制御部２２１は、メモリ部２２２に格納された指定コンテンツに対応する属性証明書（ＡＣ）を検索する。検索により抽出された属性証明書（ＡＣ）はセキュリティチップ２１０に転送され、セキュリティチップ２１０内で、属性証明書（ＡＣ）の検証処理が実行される。

【０２４６】属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップ２１０とデコーダ２８０間において相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップ２１０は、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダ２８０と共有したセッション鍵を用いてコンテンツ鍵を再暗号化し

てデコーダ２８０に送信する。暗号化コンテンツ鍵を受信したデコーダ２８０は、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【０２４７】次に、ユーザデバイス側制御部２２１は、メモリ部２２２に格納された暗号化コンテンツを検索して取り出し、デコーダ２８０に送信する。デコーダ２８０は、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【０２４８】上述したデコーダを適用した処理では、コンテンツ鍵はセキュリティチップ２１０内では使用されない。また、デコーダは、暗号化コンテンツを復号化して、アナログ出力として音声または映像データを外部出力する。なお、属性証明書（ＡＣ）には、認証するデコーダのＩＤや認証方式を記述してもよく、この場合、セキュリティチップ２１０は、相互認証時にデコーダが属性証明書（ＡＣ）に記述されたデコーダＩＤや認証方式に適合するか否かを判定して、適合する場合にのみコンテンツ鍵をデコーダに出力する。

【０２４９】デコーダを用いた処理シーケンスについて図３１を用いて説明する。図３１において、左からセキュリティチップ、上位ソフトウェア（ユーザデバイス側制御部）、デコーダの各処理を示している。

【０２５０】利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア（ユーザデバイス側制御部）に入力されると、上位ソフトウェア（ユーザデバイス側制御部）は指定コンテンツに対応するアプリケーションＩＤを取得し、アプリケーションＩＤに基づいて、ハードディスク等のメモリに格納されたアプリケーションＩＤに対応する属性証明書（ＡＣ）を検索する。

【０２５１】検索により抽出された属性証明書（ＡＣ）は、属性証明書（ＡＣ）検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、属性証明書（ＡＣ）の検証処理を実行し、属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップは、属性証明書（ＡＣ）から暗号化コンテンツ鍵を取り出して、復号化処理を実行するとともに、上位ソフトウェア（ユーザデバイス側制御部）に応答メッセージを出力する。

【０２５２】次に、セキュリティチップとデコーダ間において、上位ソフトウェア（ユーザデバイス側制御部）を介して相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップは、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共有したセッション鍵を用いてコンテンツ鍵を再暗号化してデコーダに送信する。暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【０２５３】次に、ユーザデバイス側制御部は、メモリに格納された暗号化コンテンツを検索して取り出し、デコーダに送信する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【０２５４】次に、デコーダを用いたコンテンツ復号化処理について、図３２のフローを参照して説明する。

【０２５５】ステップＳ１０１において、利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア（ユーザデバイス側制御部）に入力されると、ステップＳ１０２において、上位ソフトウェア（ユーザデバイス側制御部）は指定コンテンツに対応するアプリケーションＩＤを取得し、ステップＳ１０３において、アプリケーションＩＤに基づいて、ハードディスク等のメモリに格納されたアプリケーションＩＤに対応する属性証明書（ＡＣ）を検索する。検索により抽出された属性証明書（ＡＣ）は、ステップＳ１０４において、属性証明書（ＡＣ）検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、ステップＳ１０５において、属性証明書（ＡＣ）の検証処理を実行し、属性証明書（ＡＣ）検証処理に成功すると、セキュリティチップは、属性証明書（ＡＣ）から暗号化コンテンツ鍵を取り出して、復号化処理を実行する。また、ステップＳ１０６において、上位ソフトウェア（ユーザデバイス側制御部）に応答メッセージを出力する。

【０２５６】属性証明書（ＡＣ）検証処理に成功しなかった場合は、その後の処理は中止される。検証成功の場合は、セキュリティチップとデコーダ間において、上位ソフトウェア（ユーザデバイス側制御部）を介して相互認証およびセッション鍵の共有処理が実行される。具体的には、ステップＳ１０８において、上位ソフトウェア（ユーザデバイス側制御部）からセキュリティチップに第１認証コマンドが発行され、ステップＳ１０９においてセキュリティチップからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信し、さらに、ステップＳ１１０において、上位ソフトウェア（ユーザデバイス側制御部）からデコーダに第２認証コマンドが発行され、ステップＳ１１１においてデコーダからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信し、さらに、ステップＳ１１２において、上位ソフトウェア（ユーザデバイス側制御部）からセキュリティチップに第３認証コマンドが発行され、ステップＳ１１３においてセキュリティチップからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信する処理によって、セキュリティチップによるデコーダの認証処理が実行される。認証処理が失敗した場合（Ｓ１１４でＮＧ）は、その後の処理は中止され、成功した場合は、ステップＳ１１５に進む。

【０２５７】ステップＳ１１５において、上位ソフトウェア（ユーザデバイス側制御部）からデコーダに第４認

証コマンドが発行され、ステップＳ１１６においてデコーダからの応答を上位ソフトウェア（ユーザデバイス側制御部）が受信する。この処理によって、デコーダによるセキュリティチップの認証の成否が判定される。認証処理が失敗の場合（Ｓ１１７でＮＧ）は、その後の処理は中止され、成功した場合は、ステップＳ１１８に進む。

【０２５８】ステップＳ１１８において、セキュリティチップは、属性証明書（ＡＣ）から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共有したセッション鍵を用いてコンテンツ鍵を再暗号化（Ｓ１１８）して、上位ソフトウェア（ユーザデバイス側制御部）に送信（Ｓ１１９）する。上位ソフトウェア（ユーザデバイス側制御部）は、受信した暗号化コンテンツ鍵をデコーダに送信（Ｓ１２０）する。

【０２５９】暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得（Ｓ１２１）する。上位ソフトウェア（ユーザデバイス側制御部）は、メモリに格納された暗号化コンテンツを検索（Ｓ１２２）して取り出し、デコーダに送信（Ｓ１２３）する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行（Ｓ１２４）する。

【０２６０】このように、デコーダを用いた復号化処理においては、セキュリティチップとデコーダ間の相互認証が実行されて、相互認証の成立を条件として、セッション鍵で暗号化したコンテンツ鍵がデコーダに出力する構成としたので、信頼される機器においてのみ復号が実行され、正当なコンテンツ利用を確保することができる。

【０２６１】［コンテンツの利用制限］先に説明したように、コンテンツの利用制限情報を格納したコンテンツ対応の属性証明書中の属性情報フィールドに格納されるコンテンツ利用条件関連情報には、サービスプロバイダの提供するコンテンツの利用制限回数、利用期限等の様々な利用条件が含まれる。すなわち、以下の情報である。条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報
有効期限：期間制限の場合の有効期限情報
利用制限回数：回数制限の場合の利用可能回数

【０２６２】コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとするコンテンツに対応する属性証明書は、上記条件が買い切りとして設定される。利用期間を設定したコンテンツに対応する属性証明書は、上記条件が期間制限として設定され、有効期限が設定される。利用回数制限を設定したコンテンツに対応する属性証明書は、上記条件が回数制限として設定され、利用制限回数に設定値（回数値）が設定される。なお、回数制限処理の場合には、ユーザデバイス内で利用可能回数を管理してコンテンツ利用を実行するオフライン回数制限と、サービスプロバイダにおいて回数検証をした後、属性証明書に記録された設定回数以内のコンテンツ利用を許可するオンライン回数制限がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツが利用される。これらの具体的な処理態様について、以下、説明する。

【０２６３】ユーザデバイスにおいてコンテンツを利用するためには、利用対象となるコンテンツに対応する属性証明書中から暗号化コンテンツ鍵を取り出して復号化処理を実行してコンテンツ鍵：Ｋｃを取得することが必要となる。このコンテンツ鍵の取得処理には、デバイスのセキュリティチップ内で実行するオフライン処理、サービスプロバイダに属性証明書を送付して復号を依頼するオンライン処理があることは先に述べた通りである。属性証明書に記載されたコンテンツの利用条件に従ったコンテンツ利用処理においても、利用条件をユーザデバイス内で確認するオフライン処理、サービスプロバイダでの確認を必要とするオンライン処理がある。これらのどちらを適用するかは、属性証明書の属性情報フィールドの記載に従って決定する。

【０２６４】図３３にコンテンツ利用時におけるユーザデバイスで実行される属性証明書（ＡＣ）の利用処理フローを示す。処理フローの各ステップについて説明する。

【０２６５】ユーザデバイスは、利用対象コンテンツに対応する属性証明書をアプリケーションＩＤ（コンテンツ識別情報）に基づいて選択すると、まず、属性証明書のフォーマット確認処理を実行（Ｓ２０１）する。属性証明書に必要事項が記録され、証明書の有効期限が有効であるか等である。フォーマット確認処理が済むと、ステップＳ２０２において署名検証が実行される。先にも説明したように属性証明書には、属性証明書発行者（例えばサービスプロバイダ）の電子署名が付加されており、ユーザデバイスは、属性証明書発行者の公開鍵証明書から公開鍵を取り出して署名検証処理（図２０参照）を行なう。なお、この際使用する公開鍵証明書の検証、連鎖的公開鍵証明書の検証処理も必要に応じて実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２６６】ステップＳ２０２の署名検証処理過程において、検証が成立し、属性証明書に改竄がないと判定された場合はステップＳ２０３に進む。一方、ステップＳ２０２の署名検証処理過程において、検証が非成立となり、属性証明書に改竄ありと判定された場合は、ステップＳ２０５に進み、その属性証明書を適用した処理は実行されず、以降の処理、すなわちコンテンツ利用処理が中止される。

【０２６７】属性証明書に改竄がないと判定され、ステップＳ２０３に進むと、属性証明書内の属性情報フィールド内のコンテンツ利用条件情報を取得する。すなわち、オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかである。この条件に従って、ステップＳ２０４のオンライン処理であるか、オフラインである場合は、ステップＳ２０６において買い切りか、回数制限であるかが判定される。

【０２６８】ステップＳ２０４において、オンライン利用であると判定されると、先に図２６を用いて説明したと同様、属性証明書をサービスプロバイダに送付して属性証明書内の利用制限情報の検証が実行される。オンライン処理の場合は、期間制限、または回数制限のいずれかであり、サービスプロバイダはこれらのコンテンツ利用条件情報を属性証明書から取得して利用制限内のコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を行なう。利用制限を超えたコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を実行せず、コンテンツ利用不可であるメッセージをユーザデバイスに送信する。

【０２６９】また、ステップＳ２０４において、オフライン利用であると判定され、ステップＳ２０６で買い切りコンテンツであると判定された場合には、属性証明書には、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵に対応するサービスプロバイダ（ＳＰ）対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋで暗号化されたコンテンツ鍵データ：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］が格納されており、ユーザデバイスでは、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得して、コンテンツの復号によりコンテンツを利用する。

【０２７０】さらに、ステップＳ２０４において、オフライン利用であると判定され、ステップＳ２０６で回数制限のコンテンツであると判定された場合には、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行して、コンテンツ利用の可否判定を実行した後、利用可であるとの判定結果の取得を条件として、属性証明書内に格納された暗号化コンテンツ鍵の復号化処理を実行し、かつ、デバイス内で管理するコンテンツ利用回数管理データの更新処理等を実行する。このためにデバイス内にコンテンツ利用回数の管理データを持つことが必要となる。

【０２７１】ステップＳ２０７の利用回数管理データのインポート処理は、コンテンツ利用回数の管理データ生成処理である。なお、利用回数管理データのインポート処理は、属性証明書に基づいて実行される。コンテンツ利用回数の管理態様には、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。これらの詳細については後述する。ステップＳ２０８の属性証明書適用完了メッセージ生成ステップは、上述のＳ２０７の利用回数管理データのインポート処理が完了したことをセキュリティチップからセキュリティチップ外のユーザデバイスに通知する処理である。

【０２７２】以下、属性証明書（ＡＣ）に記載されたコンテンツ利用条件を以下の４態様に区別して、順次、説明する。

（Ａ）オンライン－利用期間制限コンテンツ
（Ｂ）オンライン－利用回数制限コンテンツ
（Ｃ）オフライン－買い切りコンテンツ
（Ｄ）オフライン－利用回数制限コンテンツ

【０２７３】（Ａ）オンライン－利用期間制限コンテンツ

まず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３４のシーケンス図に従って説明する。

【０２７４】図３４に示す処理シーケンスは、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０２７５】図３４では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ｃ）の相互認証処理、（ｄ）のコンテンツ取得処理は共通に実行される。

【０２７６】まず、（ａ）の処理から説明する。（ａ１）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索をセキュリティチップ制御部に要求する。（ａ２）セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイス制御部に出力し、（ａ３）ユーザデバイスでは付属のブラウザによりリストを表示する。（ａ４）ユーザは表示されたリストから利用予定コンテンツに対応する

属性証明書（ＡＣ）を指定し、読み出し命令をセキュリティチップ制御部に送信する。（ａ５）セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、（ａ６）ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０２７７】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、（ｂ）の処理となる。（ｂ１）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索を実行し、（ｂ２）ユーザデバイスでは付属のブラウザにより表示されたＡＣリストから利用予定コンテンツに対応する属性証明書（ＡＣ）を指定し、（ｂ３）読み出して属性証明書を表示し、（ｂ４）属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０２７８】上記（ａ）、（ｂ）のいずれかの処理によって取得されたサービスプロバイダ識別子（ＳＰ　ＩＤ）は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子（ＳＰ　ＩＤ）に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図３４の（ｃ１）に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【０２７９】この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、図３４（ｄ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０２８０】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限である。

【０２８１】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０２８２】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２８３】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０２８４】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利用条件データ、有効期限データを確認する。属性証明書に記録されている利用条件としての有効期限内のコンテンツ利用要求であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：Ｋｃの暗号化データ：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号を実行する。

【０２８５】サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。さらに、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０２８６】（ｄ５）セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティ

チップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０２８７】（ｄ６）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｄ７）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｄ８）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｄ９）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０２８８】これらの処理によって、サービスプロバイダによる属性証明書（ＡＣ）に基づく利用期間の確認処理が行われ、制限された利用期間内である場合にのみ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０２８９】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０２９０】（Ｂ）オンライン一利用回数制限コンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３５のシーケンス図に従って説明する。

【０２９１】図３５に示す処理シーケンスは、先に説明した図３４の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０２９２】図３５に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理と、（ｃ）の相互認証処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ｃ）の相互認証が成立すると、次に、図３５（ｄ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０２９３】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限である。

【０２９４】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０２９５】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０２９６】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利

用条件データ、利用制限回数を確認する。利用可能回数は、サービスプロバイダ内のデータベースに格納されており、サービスプロバイダでは、データベース内の管理データを参照して属性証明書に記録された回数制限内のコンテンツ利用であるか否かを判定する。

【０２９７】属性証明書に記録された回数制限内のコンテンツ利用であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：Ｋｃの暗号化データ：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号を実行する。サービスプロバイダは、自己の所有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋを用いて、属性証明書に格納された暗号化コンテンツ鍵：［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］の復号化処理を実行し、コンテンツ鍵：Ｋｃを取り出す。

【０２９８】さらに、サービスプロバイダは、データベース内のコンテンツ利用回数管理データを更新し、利用対象コンテンツの対応する利用可能回数を１デクリメントする処理を行なう。さらに、サービスプロバイダでは、取り出したコンテンツ鍵：Ｋｃを先の相互認証処理において生成したセッションキー（Ｋｓｅｓ）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【０２９９】（ｄ５）セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、［Ｋｓｅｓ（Ｋｃ）］を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０３００】（ｄ６）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｄ７）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｄ８）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｄ９）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０３０１】これらの処理によって、サービスプロバイダによる属性証明書（ＡＣ）に基づくコンテンツ利用回数の確認処理が行われ、制限された利用回数内である場合にのみ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０３０２】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０３０３】（Ｃ）オフライン－買い切りコンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、買い切りコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図３６のシーケンス図に従って説明する。

【０３０４】図３６に示す処理シーケンスは、先に説明した図３４、図３５の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３０５】図３６に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ａ）、（ｂ）のいずれかの処理によって、サービスプロバイダＩＤが取得されると、次に、図３６（ｃ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０３０６】（ｃ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オフライン買い切りである。

【０３０７】（ｃ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求

を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３０８】（ｃ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０３０９】（ｃ４）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｃ５）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｃ６）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｃ７）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０３１０】これらの処理によって、属性証明書（ＡＣ）に基づく買い切りコンテンツであることの確認処理が行われ、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０３１１】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【０３１２】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０３１３】（Ｄ）オフライン－利用回数制限コンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数の制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理について説明する。属性証明書の利用条件がオフライン利用で、回数制限のあるコンテンツである場合、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行するために、デバイス内にコンテンツ利用回数の管理データを持つことが必要となる。コンテンツ利用回数の管理データの保有処理が利用回数管理データのインポート処理である。

【０３１４】（Ｄ－１）インポート処理

まず、利用回数管理データのインポート処理について説明する。コンテンツ利用回数の管理態様には、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。

【０３１５】最初に図３７を参照して、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図３７の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オフライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【０３１６】（１）属性証明書がサービスプロバイダから発行され、送信されると、（２）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３１７】（３）セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。なお、ユーザがユーザデバイスにログインしている場合には、ユーザＩＤ等は保持されているので、ユーザＩＤ、サービスプロバイダＩＤはユーザが入力する代わりにユーザデバイスが送信してもよい。

【０３１８】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。図３８にセキュリティチップ内のメモリのサービスプロバイダ管理領域内に設定されるコンテンツ利用回数管理データの構成例を示す。

【０３１９】図３８に示すように、サービスプロバイダ管理領域には、サービスプロバイダＩＤ、ユーザＩＤ毎に、コンテンツ識別子としてのアプリケーションＩＤ（Ａｐｐ．ＩＤ＃ｎ）、対応する属性証明書（ＡＣ）の識別子であるＡＣシリアル（ＡＣ Ｓｅｒｉａｌ＃ｎ）、さらに残りの利用可能回数データ（Ｃｏｕｎｔ＃ｎ）が対応付けられて格納される。同一のコンテンツであっても利用ユーザ毎に異なる属性証明書に基づく利用回数カウントを可能としたデータ構成となっている。

【０３２０】図３７に戻って利用回数管理データのインポート処理のシーケンスについて説明を続ける。（３）セキュリティチップの制御部は、属性証明書から取得したコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データ、ユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証し、コンテンツ利用回数管理データが登録されていないことを確認すると、（４）コンテンツ利用回数管理データをサービスプロバイダ管理領域に追加登録し、（５）追加登録の終了後、属性証明書受信メッセージを生成して、サービスプロバイダに送信する。

【０３２１】図３７の例では、サービスプロバイダから受領した属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００１
属性証明書（ＡＣ）シリアル：１３４５
コンテンツ利用制限回数：５
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３２２】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図３７に示すＳＰ管理領域データ（更新前）のデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５に対応するデータは存在しない。

【０３２３】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理データをサービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の下段に示すＳＰ管理領域データ（更新後）のデータ中に、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：５が設定される。

【０３２４】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行され、利用可能回数が０となった以後のコンテンツ利用が拒否され、属性証明書に記録された利用制限回数内でのコンテンツ利用が可能となる。このコンテンツ利用処理については、後述する。

【０３２５】なお、サービスプロバイダから受領した属性証明書のアプリケーションＩＤ、属性証明書（ＡＣ）シリアルと同一のデータがすでに、対応するサービスプロバイダＩＤ、ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みで

ある場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【０３２６】また、サービスプロバイダから受領した属性証明書のアプリケーションＩＤと同一であるが、属性証明書（ＡＣ）シリアルが異なるデータがすでに、対応するサービスプロバイダＩＤ、ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録を実行する。

【０３２７】すなわち、同一のサービスプロバイダＩＤ、同一ユーザＩＤのサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして、すでに、例えば
アプリケーションＩＤ：０００１、
ＡＣシリアル：０００１
残りコンテンツ利用回数：２
のデータが存在する場合であっても、

【０３２８】アプリケーションＩＤ：０００１
ＡＣシリアル：０００２
残りコンテンツ利用回数：５
の新たな管理データが追加登録される。

【０３２９】図３９に、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合のセキュリティチップ内で実行される利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【０３３０】まず、ステップＳ２２１において、属性証明書（検証済み）からアプリケーションＩＤ、利用制限回数、属性証明書シリアル番号を取り出す。ステップＳ２２２において、セキュリティチップ内のメモリに設定済みのサービスプロバイダ管理領域内に、属性証明書に格納されたと同一のアプリケーションＩＤの回数管理データがあるか否かを検索する。

【０３３１】ステップＳ２２３で、同一のアプリケーションＩＤの回数管理データの登録がないと判定された場合は、ステップＳ２２５に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データ登録を行なう。

【０３３２】一方、ステップＳ２２３において、同一のアプリケーションＩＤの回数管理データが登録済みと判定された場合は、ステップＳ２２４に進み、さらに、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みでないと判定した場合は、ステップＳ２２５に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数データとして、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データの登録を行なう。

【０３３３】次に、図４０を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図４０の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オフライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【０３３４】この処理態様は、セキュリティチップ内の限られたメモリ領域を有効に活用する構成であり、回数管理データの実データファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、この外部管理ファイル情報のハッシュ（Ｈａｓｈ）値を、セキュリティチップ内部で管理することで、外部管理ファイル情報の改竄を検証することを可能としたものである。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣがハッシュ値となる。

【０３３５】図４０に示す処理シーケンスについて説明する。（１）属性証明書がサービスプロバイダから発行され、送信されると、（２）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケ

ンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３３６】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図ではユーザデバイス制御部の管理するＨＤＤに回数管理ファイルがあり、（３）ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【０３３７】次に、セキュリティチップの制御部は、（４）ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のＲＡＭに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダＩＤとユーザＩＤに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダＩＤとユーザＩＤに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【０３３８】セキュリティチップの制御部は、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルから、ユーザにより指定されているサービスプロバイダＩＤ、ユーザＩＤに対応するフィールドデータを抽出してハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【０３３９】図の例では、ＲＡＭ展開データの、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のハッシュ値：２９０ａと比較することになる。

【０３４０】（５）ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイス制御部に送信し、一致が得られなかった場合はエラーメッセージをユーザデバイス制御部に送信する。（６）次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。

【０３４１】コンテンツ利用回数管理データが登録されていないことを確認すると、（７）コンテンツの利用回数管理データを属性証明書（ＡＣ）から取り出し、ＲＡＭに展開した回数管理ファイルに追加登録し、（８）追加データに基づく新たなハッシュ値を計算して、（９）セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。（１０）追加登録の終了後、属性証明書受信メッセージを更新した回数管理ファイルとともに、ユーザデバイスに送信し、（１１）ユーザデバイスは、受信した回数管理ファイルをハードデイスクに格納する。

【０３４２】図４０の例では、サービスプロバイダから受領した属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００１
属性証明書（ＡＣ）シリアル：１３４５
コンテンツ利用制限回数：５
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３４３】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。図４０に示す最上段のＳＣ内ＲＡＭのデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５に対応するデータは存在しない。

【０３４４】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理データをサービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の中段に示すＳＣ内ＲＡＭのデータ中に、アプリケーションＩＤ：０００１、属性証明書（ＡＣ）シリアル：１３４５の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：５が設定される。

【０３４５】さらに、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するフィールドデータ

に基づいてハッシュ値が算出される。図の例では、データ更新前のハッシュ値は２９０ａであり、データ更新後のハッシュ値が８７３１であり、図の最下段のＳＰ管理領域のハッシュ値：８７３１が更新値として格納されることになる。

【０３４６】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行されるとともに、更新データに基づいて新たなハッシュ値が算出されて、更新処理が実行されることになる。このコンテンツ利用処理については、後述する。

【０３４７】なお、サービスプロバイダから受領した属性証明書のアプリケーションＩＤ、属性証明書（ＡＣ）シリアルと同一のデータがすでに、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルの対応するサービスプロバイダＩＤ、ユーザＩＤのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【０３４８】また、サービスプロバイダから受領した属性証明書のアプリケーションＩＤと同一であるが、属性証明書（ＡＣ）シリアルが異なるデータがすでに、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルの対応するサービスプロバイダＩＤ、ユーザＩＤのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録、ハッシュ値更新処理を実行する。

【０３４９】図４１に、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【０３５０】まず、ステップＳ２４１において、外部メモリから回数管理ファイルを読み込み、ステップＳ２４２において、サービスプロバイダＩＤ、ユーザＩＤに基づいて特定されるフィールドデータに基づくハッシュ値を算出し、算出ハッシュ値と、セキュリティチップのメモリ内のサービスプロバイダ管理領域に格納ずみのハッシュ値と一致するか否かを検証（Ｓ２４３）する。一致しない場合は、外部メモリから読み出した回数管理ファイルが改竄されていると判定し、エラー処理、例えばその後の処理を中止する。

【０３５１】ハッシュ値が一致し、外部メモリから読み出した回数管理ファイルが改竄されていないと判定した場合は、ステップＳ２４４に進み、属性証明書（検証済み）からアプリケーションＩＤ、利用制限回数、属性証明書シリアル番号を取り出す。次に、ステップＳ２４５において、ユーザデバイス制御部から受信し、ＲＡＭに展開した回数管理ファイルに、属性証明書に格納されたものと同一のアプリケーションＩＤの回数管理データがあるか否かを検索する。

【０３５２】ステップＳ２４６で、同一のアプリケーションＩＤの回数管理データの登録がないと判定された場合は、ステップＳ２４７に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データの登録を行なう。

【０３５３】一方、ステップＳ２４６において、同一のアプリケーションＩＤの回数管理データの登録が登録済みと判定された場合は、ステップＳ２５１に進み、さらに、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書（ＡＣ）シリアルと一致する回数管理データがＲＡＭに展開した回数管理ファイルに登録済みでないと判定した場合は、ステップＳ２４７に進み、属性証明書に従ってアプリケーションＩＤ：ｎｎｎｎ、属性証明書（ＡＣ）シリアル：ｍｍｍｍ、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：ｘを設定して利用回数管理データ登録を行なう。

【０３５４】ステップＳ２４７において、属性証明書に従って、新たな回数管理データが、ＲＡＭに展開した回数管理ファイルに書き込まれると、ステップＳ２４８において、新規追加データを含めたデータに基づいて新たなハッシュ値が計算され、新たなハッシュ値をセキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。さらに、ステップＳ２４９において、更新した回数管理ファイルに基づいて外部メモリ（例えばハードディスク）に格納された回数管理ファイルの更新が実行される。

【０３５５】次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数制限コンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図４２のシーケンス図に従って説明する。

【０３５６】図４２に示す処理シーケンスは、先に説明した図３４、図３５、図３６の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであ

るユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３５７】図４２に示す処理中、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ａ）、（ｂ）の各処理は、図３４を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。（ａ）、（ｂ）のいずれかの処理によって、サービスプロバイダＩＤが取得されると、次に、図４２（ｃ）に示す処理、すなわちコンテンツ取得処理を実行する。

【０３５８】（ｃ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オフライン利用回数制限である。

【０３５９】（ｃ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０３６０】（ｃ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、回数管理データの更新処理を実行する。回数管理データの更新処理の詳細については、後述する。さらに、セキュリティチップ制御部は、（ｃ４）属性証明書内に格納された暗号化コンテンツ鍵：［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を取り出して、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを適用して復号化処理を実行し、コンテンツ鍵：Ｋｃを取得する。コンテンツ鍵：Ｋｃの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【０３６１】（ｃ５）次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ［Ｋｃ（Ｃｏｎｔｅｎｔ）］をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、（ｃ６）セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Ｋｃを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、（ｃ７）ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、（ｃ８）セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Ｋｃ、およびコンテンツ（Ｃｏｎｔｅｎｔ）を破棄する。

【０３６２】これらの処理によって、属性証明書（ＡＣ）に基づくコンテンツの利用回数制限内のコンテンツ利用である場合に限り、コンテンツ鍵：Ｋｃがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【０３６３】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にＳＰ対応ストレージ公開鍵：ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋを用い、コンテンツ鍵の復号にＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋを用いる。この場合、ＳＰ対応ストレージ鍵（共通鍵）：ＳＣ．Ｓｔｏ．ＳＰ．Ｋは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【０３６４】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（ＡＣ：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（ＡＣ）を作成して配信することになる。

【０３６５】次に、図４３、図４４を参照して、利用回数管理データの更新処理について説明する。コンテンツ利用可能回数の管理態様には、前述したようにコンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティ

チップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する２つの態様がある。図４３は前者、図４４は後者の態様における回数管理データの更新処理シーケンスを説明する図である。

【０３６６】最初に図４３を参照して、コンテンツ利用可能回をユーザデバイス内のセキュリティチップで管理する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図４３の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【０３６７】（１）セキュリティチップの制御部は、検証済みの属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。

【０３６８】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。

【０３６９】図４３に示す例では、属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００２
属性証明書（ＡＣ）シリアル：３２７８
コンテンツ利用制限回数：１０
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３７０】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図４３に示すＳＰ管理領域データ（更新前）のデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータが存在し、利用可能回数（残回数）：７と設定されている。

【０３７１】（２）セキュリティチップ制御部は、この抽出データから利用可能回数（残回数）：７＞０であること、さらに、属性証明書に記録された制限回数以下、１０≧７であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された（３）暗号化コンテンツ鍵の復号化処理を実行する。

【０３７２】（４）さらに、セキュリティチップ制御部は、メモリ内の対応するサービスプロバイダ管理領域の対応データの利用可能回数を１減少させるデータ更新処理を実行する。この場合は、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータ中の、利用可能回数（残回数）：７を６に更新する処理を実行する。なお、（３）の暗号化コンテンツ鍵の復号化処理と、（４）の回数管理データの更新処理は、処理手順を（４）を先に（３）を後にする構成としてもよく、また並列に実行してもよい。

【０３７３】次に、図４４を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図４４の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【０３７４】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図ではユーザデバイス制御部の管理するＨＤＤに回数管理ファイルがあり、（１）ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【０３７５】次に、セキュリティチップの制御部は、
（２）ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のＲＡＭに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダＩＤとユーザＩＤに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダＩＤとユーザＩＤに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【０３７６】セキュリティチップの制御部は、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルから、ユーザにより指定されているサービスプロバイダＩＤ、ユーザＩＤに対応するフィールドデータを抽出し

てハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【０３７７】図の例では、ＲＡＭ展開データの、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７のハッシュ値：８７３１と比較することになる。

【０３７８】（３）ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイスに送信し、一致が得られなかった場合はエラーメッセージをユーザデバイスに送信する。（４）次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザＩＤ、サービスプロバイダＩＤの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションＩＤ、属性証明書（ＡＣ）シリアル番号、ユーザＩＤの各データに対応するコンテンツ利用回数管理データが、ユーザデバイスから受信し、ＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。

【０３７９】図４４に示す例では、属性証明書（ＡＣ）は、
アプリケーションＩＤ：０００２
属性証明書（ＡＣ）シリアル：３２７８
コンテンツ利用制限回数：１０
の各データが記録され、ユーザ入力データは、
ユーザＩＤ：６７３７
サービスプロバイダＩＤ：５６７８
である。

【０３８０】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがＲＡＭに展開した回数管理ファイルに登録済みであるか否かを検証する。図４４に示す最上段のＳＣ内ＲＡＭのデータ中には、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応するコンテンツ利用回数管理データとして、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータが存在し、利用可能回数（残回数）：７と設定されている。

【０３８１】（５）セキュリティチップ制御部は、この抽出データから利用可能回数（残回数）：７＞０であること、さらに、属性証明書に記録された制限回数以下、１０≧７であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された（６）暗号化コンテンツ鍵の復号化処理を実行する。

【０３８２】（７）さらに、セキュリティチップ制御部は、ＲＡＭに展開した回数管理ファイルの対応データの利用可能回数を１減少させるデータ更新処理を実行する。この場合は、アプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するデータ中の、利用可能回数（残回数）：７を６に更新する処理を実行する。

【０３８３】さらに、セキュリティチップ制御部は、（８）更新データに基づく新たなハッシュ値を計算して、（９）セキュリティチップ内の対応するサービスプロバイダ（ＳＰ）管理領域内に格納された対応するフィールドに格納する。図４４の例では、更新前のアプリケーションＩＤ：０００２、属性証明書（ＡＣ）シリアル：３２７８に対応するフィールドデータに基づくハッシュ値は８７３１であり、更新後の同フィールドのデータに基づくハッシュ値はｂｃ３５となり、サービスプロバイダＩＤ：５６７８、ユーザＩＤ：６７３７に対応する図の最下段のＳＰ管理領域のハッシュ値：ｂｃ３５が更新ハッシュ値として格納されることになる。

【０３８４】（１０）更新処理の終了後、更新した回数管理ファイルを、ユーザデバイス制御部に送信し、ユーザデバイス制御部は、受信した回数管理ファイルをハードデイスクに格納する。

【０３８５】このように、コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を１デクリメントして、５→４→３→２→１→０とするデータ更新が実行されるとともに、更新データに基づいて新たなハッシュ値が算出されて、更新処理が実行され、属性証明書に記録された利用制限回数内でのコンテンツ利用が可能となる。

【０３８６】以上、属性証明書のコンテンツ利用条件に従ったコンテンツの利用について説明した。なお、上記説明においては、期間制限と回数制限とを別々に説明したが、期間制限と回数制限の両制限を持つ属性証明書も可能であり、これらの場合は２つの条件に基づいてコンテンツ利用可否を判定した上で、属性証明書に設定された利用条件内の期限内、回数内のコンテンツ利用であることの確認を条件として、コンテンツ鍵の復号を行なうものとする。

【０３８７】［アップグレード処理］属性証明書には、コンテンツの利用条件として期間制限、回数制限、買い切り等の各種利用条件が設定され、これらの利用条件に基づいてセキュリティチップを持つユーザデバイスにおいてコンテンツの利用が行なわれることを説明した。次に、例えば属性証明書に設定されたコンテンツ利用制限回数の変更、あるいは期間制限の延長など、コンテンツの利用制限を変更する処理、すなわちアップグレード処

理について説明する。

【０３８８】アップグレード処理には、具体的には、以下に説明する各種の態様がある。

（１）利用回数制限をコンテンツ利用条件として記録した属性証明書の利用可能回数を増やす。例えば、１０回券を買って、５回残っていて、１０回に増やす。１０回券を買って、使い切って、１０回券に増やす。

（２）利用期間制限をコンテンツ利用条件として記録した属性証明書の利用期間を延長する。例えば、１週間後までしか使えないものを、１ヶ月後まで使えるように期間を延長する。期間が切れて使えなくなったものを、１ヶ月後まで使えるように期間を延長する。

（３）回数制限や期間制限をコンテンツ利用条件として記録した属性証明書の利用条件の変更。例えば、回数制限を期間制限に変更する。期間制限を回数制限に変更する。回数制限を買い切りに変更する。期間制限を買い切りに変更する。

（４）アルバム化アップグレード

一連のアルバム化されたコンテンツデータ、例えば１枚のＣＤあるいはＤＶＤ等に格納された複数（ｎ）のコンテンツ１～ｎ、あるいは何らかのシリーズ化されたコンテンツ１～ｎがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書１～属性証明書ｎの複数をユーザがユーザデバイス内に保持している場合、例えば、コンテンツ１に対応する属性証明書１、コンテンツ３に対応する属性証明書３、コンテンツ５に対応する属性証明書５、をユーザデバイスに保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ２，４，６～ｎのコンテンツを割引価格で一括（アルバム）購入できる。

【０３８９】属性証明書に基づくアップグレード処理には、上述した様々な態様がある。このアップグレード処理の実行シーケンスの概略は、次の通りである。まず、サービスプロバイダ（ＳＰ）がアップグレードメニューをユーザデバイスに提示し、ユーザがアップグレードメニューを選択する。ユーザデバイスは、ユーザの指定に従って、アップグレード処理対象とする取得済みの属性証明書の指定データとともに、アップグレード要求コマンドをセキュリティチップに送信する。セキュリティチップの制御部は、サービスプロバイダとの通信を実行して、アップグレード処理対象とする取得済みの属性証明書をサービスプロバイダに送信する。サービスプロバイダは、受信した属性証明書を検証した後、ユーザの指定したアップグレード処理を実行し、新たな属性証明書を発行しセキュリティチップに送信する。ユーザデバイスでは、新たな属性証明書の利用条件に従ってコンテンツを利用することが可能となる。

【０３９０】以下、アップグレードのベースとして用いる属性証明書（ＡＣ）に記載されたコンテンツ利用条件が以下の３態様である場合のアップグレード処理について、順次、説明する。

（Ａ）オンライン一利用期間制限コンテンツ

（Ｂ）オンライン一利用回数制限コンテンツ

（Ｃ）オフライン一利用回数制限コンテンツ

【０３９１】（Ａ）オンライン一利用期間制限属性証明書（ＡＣ）をベースとしたアップグレード処理

まず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間制限が設定された属性証明書を保有する場合、このオンライン一利用期間制限属性証明書をベースとしたアップグレード処理を図４５のシーケンス図に従って説明する。図４５には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０３９２】図４５では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、これら（ａ），（ｂ）は属性証明書の格納位置に応じて選択的に実行する。（ｃ）の相互認証処理、（ｄ）のコンテンツ取得処理は共通に実行される。

【０３９３】まず、（ａ）の処理から説明する。（ａ１）ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索をセキュリティチップ制御部に要求する。（ａ２）セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイス制御部に出力し、（ａ３）ユーザデバイスでは付属のブラウザによりリストを表示する。（ａ４）ユーザは表示されたリストからアップグレード処理対象の属性証明書（ＡＣ）を指定し、読み出し命令をセキュリティチップ制御部に送信する。（ａ５）セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、（ａ６）ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０３９４】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、（ｂ）の処理となる。（ｂ１）ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索を実行し、（ｂ２）ユーザデバイスでは付属のブラウザにより表示されたＡＣリストからアップグレード処理対象の属性証明書（ＡＣ）を指定し、読み出して属性証明書を表示し、（ｂ４）属性証明書格納データ中のサービスプロバイダ識別子（ＳＰ　ＩＤ）を取得する。

【０３９５】上記（ａ）、（ｂ）のいずれかの処理によって取得されたサービスプロバイダ識別子（ＳＰ　ＩＤ）は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子（ＳＰ　ＩＤ）に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図４５の（ｃ１）に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【０３９６】この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、図４５（ｄ）に示す処理、すなわちアップグレード属性証明書取得処理を実行する。

【０３９７】（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限であり、ユーザの指定するアップグレード条件は、例えば、

期間制限の変更（延長）
期間制限→オンライン回数制限へ変更
期間制限→オフライン回数制限へ変更
期間制限→買い切りへ変更

等の条件である。

【０３９８】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０３９９】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４００】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０４０１】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４０２】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４０３】なお、アップグレードの態様は、前述したように、

期間制限の変更（延長）
期間制限→オンライン回数制限へ変更
期間制限→オフライン回数制限へ変更
期間制限→買い切りへ変更

のいずれかであり、期間制限の変更の場合は、利用期間を新たに設定したアップグレード属性証明書を生成する。また、オンラインまたはオフライン回数制限へ変更する場合は、利用制限回数を格納したアップグレード属性証明書を生成する。また、買い切りへ変更する場合は、コンテンツ利用条件を買い切りとしたアップグレード属性証明書を生成する。

【０４０４】期間制限の変更、あるいはオンライン回数制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］として格納するが、オフライ

ン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納する。

【０４０５】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４５のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４０６】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４０７】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４０８】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４０９】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データのインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４１０】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４１１】（Ｂ）オンライン－利用回数制限属性証明書（ＡＣ）をベースとしたアップグレード処理

次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオンライン－利用回数制限属性証明書をベースとしたアップグレード処理を図４６のシーケンス図に従って説明する。図４６には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０４１２】図４６では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０４１３】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限であり、ユーザの指定するアップグレード条件は、例えば、

利用可能回数の変更（回数増加）
オンライン回数制限→期間制限へ変更
オンライン回数制限→オフライン回数制限へ変更
オンライン回数制限→買い切りへ変更
等の条件である。

【０４１４】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４１５】（ｄ３）属性証明書の検証により、属性証

明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵：ＳＰ．Ｓｔｏ．Ｋで暗号化されたコンテンツ鍵のデータ、すなわち、［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］が格納されている。

【０４１６】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４１７】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４１８】なお、アップグレードの態様は、前述したように、
利用制限回数の変更（回数増加）
オンライン回数制限→期間制限へ変更
オンライン回数制限→オフライン回数制限へ変更
オンライン回数制限→買い切りへ変更
のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報を格納したアップグレード属性証明書を生成する。

【０４１９】オンライン回数制限として利用制限回数を変更する場合、期間制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］として格納するが、オフライン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納する。

【０４２０】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４６のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４２１】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４２２】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４２３】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４２４】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４２５】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４２６】（Ｃ）オフライン－利用回数制限属性証明書（ＡＣ）をベースとしたアップグレード処理
次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオフライン－利用回数制限属

性証明書をベースとしたアップグレード処理を図４７のシーケンス図に従って説明する。図４７には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【０４２７】図４７では、最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０４２８】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オフライン回数制限であり、ユーザの指定するアップグレード条件は、例えば、

利用可能回数の変更（回数増加）
オフライン回数制限→期間制限へ変更
オフライン回数制限→オンライン回数制限へ変更
オフライン回数制限→買い切りへ変更

等の条件である。

【０４２９】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４３０】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオフライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］が格納されている。

【０４３１】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４３２】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４３３】なお、アップグレードの態様は、前述したように、

利用制限回数の変更（回数増加）
オフライン回数制限→期間制限へ変更
オフライン回数制限→オンライン回数制限へ変更
オフライン回数制限→買い切りへ変更

のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報を格納したアップグレード属性証明書を生成する。

【０４３４】オフライン回数制限として利用制限回数を変更する場合、買い切りへ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］として格納するが、期間制限へ変更、またはオンライン回数制限へ変更する場合は、元の属性証明書とは異なり、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］とする。

【０４３５】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有

していない場合は、図４７のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４３６】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４３７】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４３８】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４３９】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４４０】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４４１】（Ｄ）アルバム購入型アップグレード

次に、一連のアルバム化されたコンテンツデータ、例えば１枚のＣＤあるいはＤＶＤ等に格納された複数（ｎ）のコンテンツ１～ｎ、あるいは何らかのシリーズ化されたコンテンツ１～ｎがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書１～属性証明書ｎの複数をユーザがユーザデバイス内に保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ２，４，６～ｎのコンテンツを割引価格で一括（アルバム）購入する処理としたアップグレード処理について、図４８を参照して説明する。

【０４４２】図４８は、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。最上段（ａ）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理、（ｂ）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダＩＤ取得処理を示し、（ｃ）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図４５の場合と同様であり、説明を省略する。

【０４４３】相互認証後成立後の処理から説明する。

（ｄ１）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書は、ある複数のコンテンツの集合対として識別されるアルバムを構成する一部のコンテンツに対応する１以上の属性証明書である。ユーザの指定するアップグレード条件は、例えば、

アルバムを構成する他の一部コンテンツの購入

アルバムを構成する他の全コンテンツの購入

等の条件である。

【０４４４】（ｄ２）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（ＡＣ）アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４４５】（ｄ３）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。

【０４４６】（ｄ４）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連

鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、（ｄ５）ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【０４４７】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【０４４８】なお、アップグレードの態様は、前述したように、

アルバムを構成する他の一部コンテンツの購入

アルバムを構成する他の全コンテンツの購入

のいずれかであり、アルバムを構成する他の一部コンテンツの購入の場合は、購入指定の一部コンテンツに対応するアップグレード属性証明書を生成する。また、アルバムを構成する他の全コンテンツの購入の場合は、アルバムを構成する他の全コンテンツに対応するアップグレード属性証明書を生成する。

【０４４９】なお、この場合の利用条件は、ユーザが予め指定することも可能であり、また、サービスプロバイダが決定する構成としてもよい。ユーザが指定する場合は、図４８のステップ（ｄ１）において指定し、（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、指定条件を併せて送付する。

【０４５０】サービスプロバイダは、オフライン利用とするアップグレード属性証明書を生成する場合は、サービスプロバイダ管理領域に格納されたＳＰ対応ストレージ秘密鍵：ＳＣ．Ｓｔｏｐｒｉ．ＳＰ．Ｋに対応する公開鍵で暗号化したコンテンツ鍵［ＳＣ．Ｓｔｏｐｕｂ．ＳＰ．Ｋ（Ｋｃ）］を格納し、オンライン利用とするアップグレード属性証明書を生成する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵［ＳＰ．Ｓｔｏ．Ｋ（Ｋｃ）］とする。

【０４５１】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたＳＰ対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図４８のステップ（ｄ３）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてＳＰ対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【０４５２】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【０４５３】（ｄ６）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【０４５４】（ｄ７）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（ｄ８）アップグレード属性証明書をメモリに格納する。

【０４５５】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図３７～図４１を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【０４５６】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップクレード属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【０４５７】［データバックアップおよびリストア処理］ユーザがサービスプロバイダから購入し、セキュリティチップを有するユーザデバイス内の記憶手段に格納した権利情報や、証明書類は、消失の事態に備えてバックアップしておくことが好ましい。バックアップすべき情報には、見られてもいい情報と、セキュアに保持しなければいけない情報がある。見られてもいい情報とは、公開鍵証明書、属性証明書などの証明書類である。セキュアに保持する情報とは、例えばセキュリティチップのサービスプロバイダ管理領域に書き込まれているサービス加入の証拠情報などがある。

【０４５８】公開鍵証明書、属性証明書などの証明書類については、ユーザが適宜、ハードディスクやフラッシュメモリを搭載したメモリカードなどに複製情報を格納しておくことで十分である。属性証明書にはコンテンツ鍵が格納されているが、オンライン利用の場合には、サ

ービスプロバイダとの接続が必要となり、この際の相互認証時にデバイス（セキュリティチップ）の正当性が確認されるので、コンテンツが不正に利用されることはない。また、オフライン利用の場合でも、コンテンツ鍵を復号するための鍵は、セキュリティチップのサービスプロバイダ管理領域に格納されているので、正当なユーザデバイスのセキュリティチップを保持し、かつ前述したパスワードによるアクセスが許可されたユーザのみが暗号化コンテンツ鍵を復号することが可能となる。従って、属性証明書が第三者に渡ったとしてもコンテンツの不正利用が発生することはない。

【０４５９】しかし、セキュリティチップ内の秘密情報に関しては、テンポラリのストレージにセキュアに保持しておかねばならない。例えばセキュリティチップのサービスプロバイダ管理領域には、サービスプロバイダとの相互認証に必要なＩＤ情報、鍵情報、パスワード等が格納されており、これらは第三者に漏洩することを防止することが必要である。従って外部の記憶媒体（テンポラリのストレージ）にバックアップする際には、これらのバックアップデータは、暗号化しておくことが必要である。

【０４６０】ユーザが秘密情報をテンポラリのストレージに格納した場合、ストレージメディアの盗難によりデータ漏洩が発生する暗号化では意味がない。また、ユーザデバイスから容易に取り出せる鍵によって復号できる構成とすると、ユーザデバイスから取り出した鍵によって、セキュリティデバイスの複製を生成することが可能となってしまい、ユーザサイドで全く同様のサービスプロバイダ管理領域データを有する第２のセキュリティデバイスを生成することが可能となるおそれがある。また、複製したセキュリティチップを搭載した可搬メディアを他のユーザデバイスに装着することで、複数のユーザデバイスで全く同様のサービスを受けることが可能となってしまう。そこで本発明のシステムでは、テンポラリのストレージに秘密情報をバックアップデータとして格納した場合でも、不正な第三者によって復号できない態様とするとともに、ユーザデバイスを保持するユーザ自身もシステムホルダの許可なくリストア等、他のセキュリティチップに格納して使用することのできない構成とし、データの復号、リストアはサポートセンタにおいてのみ実行可能とした。

【０４６１】すなわち、ユーザデバイス内で確実な情報管理を実行し、データ消失を完全に防ぐことの困難性に鑑み、本発明のシステムにおいては、サポートセンタにおいて、データのバックアップ・サービスを提供し、必要に応じてサポートセンタにおいて、バックアップデータを用いてデータ復旧、すなわちリストア処理を実行する。リストアは、サポートセンターにて行い、テンポラリのストレージからデータを読み出し、ユーザデバイスのセキュリティデバイスに対してインポートする処理として実行する。以下、サポートセンタによるデータバックアップ処理、およびリストア処理について説明する。

【０４６２】図４９に、ユーザデバイス内の秘密情報のバックアップ処理、サポートセンタにおけるリストア処理の概要を説明する図を示す。

【０４６３】図４９において、ユーザデバイス４１０は、セキュリティチップ４１１を有し、セキュリティチップには様々なシークレット、すなわち秘密情報が格納されている。秘密情報は、例えばセキュリティチップのサービスプロバイダ管理領域の格納情報であり、サービスプロバイダとの相互認証に必要なＩＤ情報、鍵情報、パスワード等である。また、ユーザデバイスのセキュリティチップ外のメモリには、公開鍵証明書、属性証明書が格納される。

【０４６４】ユーザは、ユーザデバイスの損壊、あるいはデータの消失等に備え、これらの情報をユーザデバイス以外の外部の記憶媒体にバックアップして保存する。例えば公開鍵証明書、属性証明書等を外部のＰＣのハードディスクに格納したり、フラッシュメモリを備えたカード型記憶媒体などの外部記憶媒体４２１に格納する。これらは、前述したように、漏洩により、コンテンツの不正利用を発生させるおそれがなく、暗号化されることなく外部の記憶媒体４２１に格納し、必要に応じてユーザが記憶媒体４２１からユーザデバイス４１０にリストアすることが可能である。

【０４６５】一方、セキュリティチップに格納された秘密情報は、外部の記憶媒体４２２にバックアップデータとして保存する場合は、ユーザデバイスにおいて一時的な鍵として乱数からバックアップ鍵：Ｋｂ（共通鍵系）を生成し、バックアップ鍵：Ｋｂによって、各種の秘密情報（ＳｅｃＤａｔａ）を暗号化し、暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］として記憶媒体４２２に格納する。さらに、生成したバックアップ鍵：Ｋｂをサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］を併せて外部記憶媒体４２２に格納する。秘密情報を外部の記憶媒体４２２に格納した後、バックアップ鍵：Ｋｂはユーザデバイスに保持することなく消去する。

【０４６６】記憶媒体４２２に格納した暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］は、たとえ記憶媒体４２２が第三者の手に渡ったとしても、その復号のための鍵であるバックアップ鍵：Ｋｂが、サポートセンタの公開鍵：Ｋｐｓによって暗号化されており、バックアップ鍵：Ｋｂを取得するためには、サポートセンタの秘密鍵：Ｋｓｓによる復号化処理が必要となるので、第三者による復号は不可能である。また、ユーザデバイスを保持する正当なユーザも復号により第２のセキュリティデバイスを生成することはできない。

【０４６７】データのリストア（復旧）処理は、ユーザサイト側からサポートセンタ４５０に対して記憶媒体４

２２を送付することによって実行される。リストア処理は、元のユーザデバイスが損壊した場合は、新たなユーザデバイス４３０に対して実行される。元のユーザデバイス自体をサポートセンタに送付して、修理された元のユーザデバイスに対してリストアを実行することも可能である。なお、新たなユーザデバイスに対するリストア処理を実行する場合は、元のユーザデバイスを無効化する処理、すなわちリボーク処理を併せて実行する。このリボーク処理は、例えばユーザデバイスに対応して発行されている公開鍵証明書をリボケーションリストに登録することによって行われる。リボケーションリストは、不正デバイス、無効化されたデバイス、ユーザ等に対応する公開鍵証明書のリストとして構成されるものである。リボケーションリストは、デバイスとの相互認証時に参照され、リストに記載されたデバイスであると判定されると認証を不成立として、その後のデータ通信を中止することを可能としたものである。

【０４６８】サポートセンタ４５０におけるリストア処理は、まず、ユーザサイトから送付された記憶媒体４２２’に格納されたサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］を取り出して、サポートセンタの秘密鍵：Ｋｓｓによって復号してバックアップ鍵:Ｋｂを取り出す。その後、取得したバックアップ鍵:Ｋｂを適用して、バックアップ鍵により暗号化された秘密情報暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］の復号化処理を実行し、復号データ：ＳｅｃＤａｔａをユーザデバイス４３０のセキュリティチップ内に格納する処理として実行される。具体的なリストア処理シーケンスについては、後述する。

【０４６９】上述したように、ユーザデバイス内の秘密情報のバックアップデータのリストアをサポートセンタのみにおいて実行可能とした構成により、秘密情報の複製利用を防止することが可能となる。

【０４７０】図５０にリストア処理時の手順概要を説明する図を示す。ユーザサイトでは、ユーザが使用しているユーザデバイス４７０内のセキュリティチップに格納された秘密情報をバックアップストレージメディア４７１に格納する。前述したように、ユーザデバイスは、バックアップ鍵：Ｋｂ（共通鍵系）を生成し、バックアップ鍵：Ｋｂによって秘密情報（ＳｅｃＤａｔａ）を暗号化したデータ：［Ｋｂ（ＳｅｃＤａｔａ）］と、バックアップ鍵：Ｋｂをサポートセンタの公開鍵：Ｋｐｓによって暗号化した暗号鍵データ［Ｋｐｓ（Ｋｂ）］をバックアップストレージメディア４７１に格納する。

【０４７１】ユーザデバイス４７０が損壊する等の理由により、使用できなくなった場合、ユーザは、バックアップストレージメディア４７１をサポートセンタ４７５に送付する。

【０４７２】サポートセンタ４７５は、新規のユーザデバイス、あるいは損壊したユーザデバイスを修理した元のユーザデバイスに対して、バックアップストレージメディア４７１のデータを復号してリストアし、秘密情報をリストアしたユーザデバイス４７２と、リストアに使用したバックアップストレージメディア４７１をユーザに返却する。サポートセンタ４７５は、このリストア処理において、新規デバイスに対してリストア処理を実行し、元のデバイスを使用しない場合には、前述したリボーケーションリストへの登録によるリボーク処理を実行する。またサポートセンタ４７５は、リストア処理に対する課金を実行してもよい。

【０４７３】図５１を参照して、ユーザサイトで実行するバックアップストレージメディアに対するデータバックアップ処理シーケンスについて説明する。図５１は、左からバックアップストレージメディア、ユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。まず、（１）ユーザデバイス制御部は、セキュリティチップ制御部に対してバックアップ処理要求を送信する。これは、ユーザがユーザデバイス側の入力部に対するユーザによるバックアップ処理実行指示に基づいて行われる。

【０４７４】セキュリティチップの制御部は、バックアップ要求を受信すると、（２）バックアップデータの暗号化に適用するバックアップ鍵（キー）：Ｋｂを生成する。バックアップ鍵（キー）：Ｋｂは例えば乱数生成手段によって生成した乱数に基づいて生成するバックアップ専用の一時的な鍵であり、バックアップストレージメディアに対するバックアップ処理の後、セキュリティチップに保持されることなく、消去される。

【０４７５】セキュリティチップの制御部は、（３）バックアップ鍵（キー）：Ｋｂの生成後、生成したバックアップ鍵（キー）で、バックアップデータの暗号化を行ない、暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］を生成する。データ暗号化が終了すると、さらに、（４）セキュリティチップの制御部は、バックアップ鍵（キー）：Ｋｂをサポートセンタの公開鍵：Ｋｐｓを用いて暗号化して暗号鍵データ：［Ｋｐｓ（Ｋｂ）］を生成する。

【０４７６】上記処理の後、セキュリティチップの制御部は、（５）暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］と、暗号鍵データ：［Ｋｐｓ（Ｋｂ）］をバックアップストレージメディアに格納する。なお、これらの処理の後、バックアップ鍵（キー）：Ｋｂは、セキュリティチップから消去される。

【０４７７】なお、バックアップストレージメディアに暗号化データ：［Ｋｂ（ＳｅｃＤａｔａ）］と、暗号鍵データ：［Ｋｐｓ（Ｋｂ）］を格納することなく、これらのデータを直接サポートセンタに送信し、サポートセンタ内の記憶手段にユーザデバイスＩＤ、またはセキュリティチップＩＤに対応させてバックアップデータを保存する構成としてもよい。このような構成とした場合

は、バックアップデータに基づくリストア処理は、ユーザデバイス（セキュリティチップ）側からサポートセンタに対する通信ネットワークを介したリクエストに応じて実行可能となり、バックアップストレージメディアを送付することなく、リストア処理を実行することが可能となる。

【０４７８】次に、図５２を参照して、サポートセンタで実行するバックアップストレージメディアからのバックアップデータの取得処理について説明する。サポートセンタでは、まず、ユーザサイトから送付されたバックアップストレージメデイアに格納されたデータを読み出す。読み出しデータは、バックアップ鍵（キー）：Ｋｂで暗号化されたバックアップデータ：［Ｋｂ（ＳｅｃＤａｔａ）］と、バックアップ鍵（キー）：Ｋｂをサポートセンタの公開鍵：Ｋｐｓを用いて暗号化した暗号鍵データ：［Ｋｐｓ（Ｋｂ）］である。なお、前述したように、サポートセンタ内の記憶手段にユーザデバイスＩＤ、またはセキュリティチップＩＤに対応させてバックアップデータを保存した構成とした場合は、サポートセンタは、ユーザサイトからのリストア処理リクエストに基づいて、記憶手段からこれらのデータの読み出しを行なう。

【０４７９】サポートセンタは、データの読み出しの後、まずサポートセンタの公開鍵：Ｋｐｓで暗号化したバックアップ鍵（キー）：Ｋｂデータ：［Ｋｐｓ（Ｋｂ）］を、サポートセンタの公開鍵に対応する秘密鍵：Ｋｓｓで復号化処理を実行し、バックアップ鍵（キー）：Ｋｂを取り出す。さらに、バックアップ鍵（キー）：Ｋｂで暗号化されたバックアップデータ：［Ｋｂ（ＳｅｃＤａｔａ）］を、取り出したバックアップ鍵（キー）：Ｋｂを適用して復号化処理を実行し、バックアップデータ：ＳｅｃＤａｔａを取り出す。

【０４８０】次に、図５３を参照して、サポートセンタで実行するリストア処理のシーケンスについて説明する。図５３は、左から、リストア処理によりデータを格納する新たなユーザデバイスのセキュリティチップ制御部、およびユーザデバイス制御部、サポートセンタサーバ、さらに、属性証明書発行者である属性証明書認証局（ＡＡ：Attribute Certificate Authority）の処理を示している。なお、属性証明書発行局は、属性証明書を発行する機関であり、例えばサービスプロバイダ内に構成される。ここで属性証明書発行局は、ユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ管理領域を生成するための属性証明書である。

【０４８１】前述したように、サービスプロバイダ管理領域生成用の属性証明書は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設定することを目的として発行される属性証明書であり、属性情報フィールドには、サービスプロバイダ識別子（ＩＤ）、サービスプロバイダ・ネーム、処理態様：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録される。

【０４８２】図５３の処理シーケンスについて説明する。まず、（１）ユーザデバイス制御部からセキュリティチップ制御部に対してリストア処理要求が出力される。これは、サポートセンタのオペーレータによってユーザデバイス側の入力部に対して実行するリストア処理実行指示に基づいて行われる。

【０４８３】セキュリティチップ制御部は、（２）ユーザデバイス制御部からリストア処理要求を受信すると、（３）セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図１６のＴＬＳ１．０処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（ＣＡ）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Ｋｓｅｓ）を共有する。相互認証が成立すると、次に、（４）セキュリティチップ制御部は、サポートセンタに対してリストア処理要求を送信する。

【０４８４】サポートセンタは、セキュリティチップからのリストア処理要求を受信すると、（５）バックアップデータの検索処理を行なう。これは、サポートセンタが、ユーザサイトからバックアップデータを受領済みであるか否かの確認として実行される。

【０４８５】サポートセンタは、次に、（６）メモリ領域確保用属性証明書（ＡＣ）の発行要求を属性証明書発行局（者である）に対して送信する。（７）属性証明書（ＡＣ）の発行要求を受信した属性証明書発行者である属性証明書認証局（ＡＡ）は、メモリ領域確保用属性証明書（ＡＣ）を生成する。なお、属性証明書（ＡＣ）は、予め属性証明書認証局（ＡＡ）から発行を受けておいてもよい。

【０４８６】メモリ領域確保用属性証明書は、属性情報フィールドに、サービスプロバイダ識別子（ＩＤ）、サービスプロバイダ・ネーム、処理態様：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録されたものであり、例えば各サービスプロバイダの管理の下に発行される。従って、リストア処理が１つのサービスプロバイダ管理領域内のデータについてのみ実行される場合は、１つのメモリ領域確保用属性証明書によりセキュリティチップ制御部内のメモリに１つのサービスプロバイダ管理領域が設定され、データのリストアが実行されるが、複数のサービスプロバイダ管理領域内のデータについてリストアを実行する場合は、複数のメモリ領域確保用属性証明書の発行を受けて、セキュリティチップ制御部内のメモリに複数のサービスプロバイダ管理領域を設定した上で、各利用域についてデータ格納を行なうことになる。

【０４８７】（８）属性証明書発行者である属性証明書認証局（ＡＡ）は、生成したメモリ領域確保用属性証明書（ＡＣ）をサポートセンタサーバに送信する。サポートセンタは、属性証明書発行者である属性証明書認証局（ＡＡ）からメモリ領域確保用属性証明書（ＡＣ）を受信すると、（９）属性証明書、およびバックアップデータをセキュリティチップ制御部に送信する。バックアップデータは、メモリ領域確保用属性証明書（ＡＣ）によって、セキュリティチップのメモリに確保されるサービスプロバイダ管理領域に格納するデータであり、例えば、サービスプロバイダ（ＳＰ）対応秘密鍵、サービスプロバイダ（ＳＰ）対応ストレージ秘密鍵、外部管理情報のハッシュ値、利用回数管理データ、認証情報、ユーザ情報等の各データである。

【０４８８】（１０）セキュリティチップ制御部は、サポートセンタサーバからのメモリ領域確保用属性証明書（ＡＣ）を受信すると、属性証明書の検証処理を実行する。検証処理には、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図２０の処理フローと同様のシーケンスに従って実行される。

【０４８９】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（ＡＣ）内のＡＣ保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（ＡＣ）の発行者の信頼度が不確かである場合には、属性証明書（ＡＣ）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（ＣＡ）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【０４９０】（１１）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、メモリ領域確保用属性証明書（ＡＣ）に記録された条件に従って、セキュリティチップ内のメモリにサービスプロバイダ管理領域を設定する。（１２）さらに、セキュリティチップの制御部は、メモリに設定されたサービスプロバイダ管理領域内にサポートセンタサーバから受信したバックアップデータを格納する。

【０４９１】以上の処理により、ユーザデバイスのセキュリティチップのメモリに、メモリ領域確保用属性証明書に記録された条件に従ってサービスプロバイダ管理領域が確保され、確保されたサービスプロバイダ管理領域にバックアップデータが格納される。なお、複数のサービスプロバイダ管理領域に対応するバックアップデータのリストアを行なう場合は、複数のメモリ領域確保用属性証明書の発行に基づいて同様の処理を繰り返し実行する。

【０４９２】なお、上述の処理シーケンスの後、あるいはその途中において、サポートセンタは、廃棄対象となる元のユーザデバイスのリボーク処理を実行する。さらに、リストアを要求してきたユーザに対する課金処理を実行してもよい。

【０４９３】［各エンティティの構成］次に、上述したコンテンツ利用管理システムを構成する各エンティティの構成例について図を参照しながら、説明する。まずサービスプロバイダからのコンテンツを受領するサービス受領デバイスとしてのユーザデバイスの構成例を図５４を参照して説明する。

【０４９４】ユーザデバイスはデータ処理、制御を実行するＣＰＵ、サービスプロバイダ他と通信可能な通信手段を備えたＰＣ等のデータ処理手段によって実現することができる。図５４にデバイスの構成例を示す。なお、図５４に示すデバイス構成例は１つの例であり、デバイスは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。図５４に示すＣＰＵ(Central processing Unit)５０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行するプロセッサである。ＲＯＭ（Read-Only-Memory）５０２は、ＣＰＵ５０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）５０３は、ＣＰＵ５０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【０４９５】ＨＤＤ５０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ５１２は、前述したように耐タンパ構造を持つ構成であり、暗号処理に必要な鍵データ、アクセス許可書の格納領域としてのメモリ、制御部を有する。

【０４９６】バス５１０はＰＣＩ（Peripheral Component Interface）バス等により構成され、各モジュール、入出力インタフェース５１１を介した各入手力装置とのデータ転送を可能にしている。

【０４９７】入力部５０５は、例えばキーボード、ポインティングデバイス等によって構成され、ＣＰＵ５０１に各種のコマンド、データを入力するためにユーザにより操作される。出力部５０６は、例えばＣＲＴ、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【０４９８】通信部５０７はデバイスの接続したエンティティ、例えばサービスプロバイダ等との通信処理を実行し、ＣＰＵ５０１の制御の下に、各記憶部から供給されたデータ、あるいはＣＰＵ５０１によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【０４９９】ドライブ５０８は、フロッピー（登録商

標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体５０９の記録再生を実行するドライブであり、各リムーバブル記録媒体５０９からのプログラムまたはデータ再生、リムーバブル記録媒体５０９に対するプログラムまたはデータ格納を実行する。

【０５００】各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ５０１において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース５１１、バス５１０を介して例えば接続されているＲＡＭ５０３に供給される。

【０５０１】前述の説明内に含まれるユーザデバイスにおける処理を実行するためのプログラムは例えばＲＯＭ５０２に格納されてＣＰＵ５０１によって処理されるか、あるいはハードディスクに格納されＨＤＤ５０４を介してＣＰＵ５０１に供給されて実行される。

【０５０２】次に、本発明のシステムの構成エンティティであるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局等の各エンティティを構成するデータ処理装置の構成例について説明する。これらのエンティティは例えば図５５に構成によって実現することができる。なお、図５５に示すデータ処理装置構成例は１つの例であり、各エンティティは、ここに示すべての機能を必ずしも備えることが要求されるものではない。

【０５０３】図５５に示すＣＰＵ(Central processing Unit)６０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実際に実行する。ＲＯＭ（Read-Only-Memory）６０２は、ＣＰＵ６０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）６０３は、ＣＰＵ６０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。ＨＤＤ６０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段６０５は、送信データの暗号処理、復号化処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをＲＯＭ６０２に格納し、ＣＰＵ６０１がＲＯＭ格納プログラムを読み出して実行するように構成してもよい。

【０５０４】ドライブ６０６は、フロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体６０７の記録再生を実行するドライブであり、各リムーバブル記録媒体６０７からのプログラムまたはデータ再生、リムーバブル記録媒体６０７に対するプログラムまたはデータ格納を実行する。各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ６０１において実行または処理を行なう場合は、読み出したプログラム、データはバス６１０を介して例えば接続されているＲＡＭ６０３、通信部６０８、通信部６０９に供給される。

【０５０５】通信部６０８、通信部６０９は、それぞれ異なるエンティティを通信相手として通信する処理を想定して複数の通信部を設けた例を示している。例えばサービスプロバイダであれば、一方はユーザデバイスとの通信、他方はコンテンツクリエータとの通信処理に使用される。各通信部を介して通信相手との相互認証、暗号化データの送受信処理等が実行される。

【０５０６】前述した説明内に含まれるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局を構成するデータ処理装置における各処理を実行するためのプログラムは例えばＲＯＭ６０２に格納されてＣＰＵ６０１によって処理されるか、あるいはハードディスクに格納されＨＤＤ６０４を介してＣＰＵ６０１に供給されて実行される。

【０５０７】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０５０８】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０５０９】例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０５１０】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送

したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０５１１】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０５１２】

【発明の効果】以上、説明したように、本発明のコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容しようとするシステムにおいて、サービスプロバイダが、ユーザデバイスからコンテンツ利用条件情報の変更処理要求を伴うコンテンツ利用権限証明書を受信し、受信したコンテンツ利用権限証明書に記録されたコンテンツ利用条件情報を変更したアップグレードコンテンツ利用権限証明書を生成し、ユーザデバイスに対して発行する構成としたので、ユーザ情報およびユーザのコンテンツ購入情報をコンテンツ利用権限証明書から取得することが可能となり、正当なコンテンツ利用権限を有するユーザであることの確認が確実に実行され、ユーザのコンテンツ利用権限の管理データを、サービスプロバイダ側でユーザ毎に保有することなく、正当なユーザに対するコンテンツの利用条件の変更処理を実行することが可能となる。

【０５１３】さらに、本発明のコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、コンテンツ利用期間制限の変更、またはコンテンツ利用回数制限の変更、あるいは利用期間制限、利用回数制限、買い切りの３態様間の変更の少なくともいずれかを実行してアップグレードコンテンツ利用権限証明書を生成する構成としたので、各態様の利用条件を持つコンテンツ対応のコンテンツ利用権限証明書に基づいて全く異なる条件を設定したコンテンツ利用権限証明書を発行することが可能となり、コンテンツ利用における利便性が高められる。

【０５１４】さらに、本発明のコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、オンライン利用処理、またはオフライン利用処理のいずれかの利用条件情報の変更処理を実行してアップグレードコンテンツ利用権限証明書を生成する構成としたので、各態様の利用条件を持つコンテンツ対応のコンテンツ利用権限証明書に基づいて全く異なる条件を設定したコンテンツ利用権限証明書を発行することが可能となり、コンテンツ利用における利便性が高められる。

【０５１５】さらに、本発明のコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、コンテンツ利用権限証明書に格納されたコンテンツ情報に基づいて、該コンテンツ情報と同一の集合コンテンツとして識別される同一アルバムに属するコンテンツに対応するコンテンツ利用権限証明書をアップグレードコンテンツ利用権限証明書として生成し、ユーザデバイスに対して送信する構成としたので、ユーザ情報およびユーザのコンテンツ購入情報をコンテンツ利用権限証明書から取得することが可能となり、正当なコンテンツ利用権限を有するユーザであることの確認が確実に実行され、ユーザのコンテンツ購入情報を、サービスプロバイダ側でユーザ毎に保有することなく、正当なユーザに対する新たなコンテンツの提供処理を実行することが可能となる。

【０５１６】さらに、本発明のコンテンツ利用権限管理システム、コンテンツ利用権限管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、コンテンツ利用権限証明書に、該コンテンツ利用権限証明書の発行エンティテイの電子署名を付加し、コンテンツ利用権限証明書のアップグレード処理を、電子署名の検証によりデータ改竄のないことの確認を条件として実行する構成としたので、不正な証明書を偽造して不正なコンテンツの利用が行なわれる可能性を排除できる。

【図面の簡単な説明】

【図１】本発明のコンテンツ利用管理システム構成の概要を説明する図である。

【図２】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図３】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図４】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図５】本発明のコンテンツ利用管理システムにおいて適用可能な権限情報証明書としての属性証明書のフォーマットを示す図である。

【図６】ユーザデバイスにおけるセキュリティチップの構成を示す構成図である。

【図７】ユーザデバイス内での処理対象となる主なデータを示す図である。

【図８】認証情報（パスワード）の初期登録処理シーケンスを示す図である。

【図９】認証情報（パスワード）の変更処理シーケンスを示す図である。

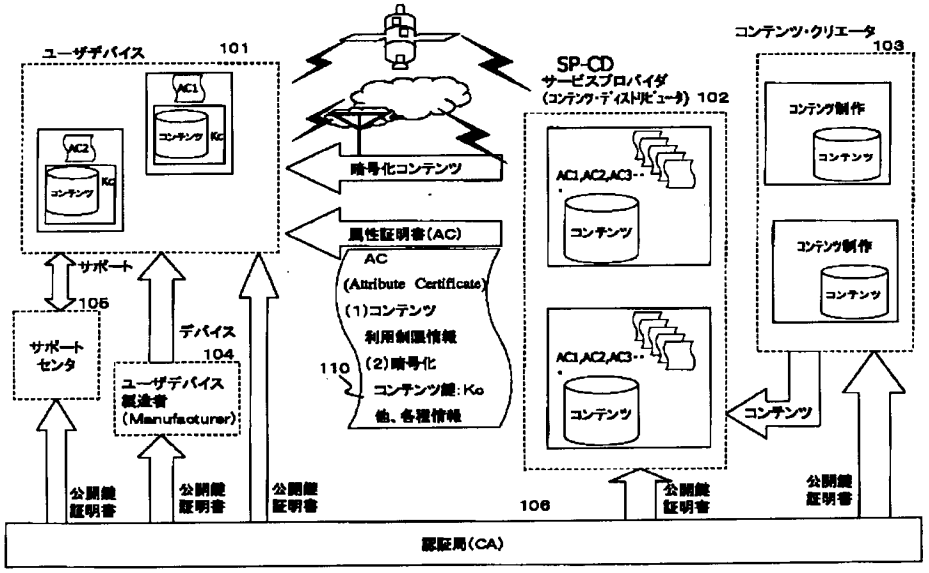
【図１０】認証情報（パスワード）の変更処理シーケンスを示す図である。
【図１１】認証情報（パスワード）とマスタパスワードとの対応について説明する図である。
【図１２】マスタパスワードの配布処理について説明する図である。
【図１３】マスタパスワードの再発行処理シーケンスを示す図である。
【図１４】マスタパスワードの算出処理を示すフロー図である。
【図１５】属性証明書（ＡＣ）発行、コンテンツ受信処理シーケンスを示す図である。
【図１６】相互認証処理の例であるＴＬＳ１．０ハンドシェイクプロトコルのシーケンスを示す図である。
【図１７】データ改竄検証に適用するＭＡＣの生成処理を説明する図である。
【図１８】属性証明書（ＡＣ）の発行処理シーケンスを示す図である。
【図１９】署名生成処理の例であるＥＣＤＳＡ署名生成手順を説明するフロー図である。
【図２０】署名検証処理の例であるＥＣＤＳＡ署名検証手順を説明するフロー図である。
【図２１】公開鍵証明書（ＰＫＣ）と属性証明書（ＡＣ）との関連付けについて説明する図である。
【図２２】公開鍵証明書（ＰＫＣ）の検証処理フローを示す図である。
【図２３】属性証明書（ＡＣ）の検証処理フロー（例１）を示す図である。
【図２４】属性証明書（ＡＣ）の検証処理フロー（例２）を示す図である。
【図２５】属性証明書（ＡＣ）を利用したコンテンツ利用処理（オフライン）を説明するシーケンス図である。
【図２６】属性証明書（ＡＣ）を利用したコンテンツ利用処理（オンライン）を説明するシーケンス図である。
【図２７】グローバル共通鍵によるコンテンツ鍵の暗号化データを格納した属性証明書（ＡＣ）を利用したコンテンツ利用処理（オフライン）を説明する図である。
【図２８】グローバル共通鍵の更新処理を説明するシーケンス図である。
【図２９】グローバル共通鍵の更新処理を説明するシーケンス図である。
【図３０】デコーダを用いた復号化処理について説明する図である。
【図３１】デコーダを用いた復号化処理シーケンスについて説明する図である。
【図３２】デコーダを用いた復号化処理フローについて説明する図である。
【図３３】ユーザデバイス側における属性証明書（ＡＣ）の適用処理を説明するフロー図である。
【図３４】属性証明書（ＡＣ）を利用したオンライン期間制限コンテンツの利用処理を説明するシーケンス図である。
【図３５】属性証明書（ＡＣ）を利用したオンライン回数制限コンテンツの利用処理を説明するシーケンス図である。
【図３６】属性証明書（ＡＣ）を利用したオフライン買い切りコンテンツの利用処理を説明するシーケンス図である。
【図３７】オフライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明する図である。
【図３８】オフライン回数制限コンテンツに対応する利用回数管理データのデータ構成例を示す図である。
【図３９】オフライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明するフロー図である。
【図４０】オフライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理を説明する図である。
【図４１】オフライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理を説明するフロー図である。
【図４２】オフライン回数制限コンテンツの属性証明書を適用したコンテンツ利用処理を説明する図である。
【図４３】オフライン回数制限コンテンツに対応する回数管理データの更新処理を説明する図である。
【図４４】オフライン回数制限コンテンツに対応するハッシュ値管理型の回数管理データの更新処理を説明する図である。
【図４５】オンライン期間制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４６】オンライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４７】オフライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。
【図４８】アルバム購入型のアップグレード処理を説明する図である。
【図４９】サポートセンタによるデータリストア処理の概要を説明する図である。
【図５０】サポートセンタによるデータリストア処理の処理シーケンス概要を説明する図である。
【図５１】ユーザデバイス側で実行するデータバックアップ処理シーケンスを説明する図である。
【図５２】サポートセンタによるバックアップデータ読み出し処理の概要を説明する図である。
【図５３】サポートセンタによるデータリストア処理シーケンスを説明する図である。
【図５４】ユーザデバイスの構成例を示す図である。
【図５５】サービスプロバイダ、サポートセンタ、コンテンツクリエータ等の各エンティティの構成例を示す図

である。

【符号の説明】

１０１　ユーザデバイス
１０２　サービスプロバイダ
１０３　コンテンツクリエータ
１０４　ユーザデバイス製造者
１０５　サポートセンタ
１０６　認証局
１１０　属性証明書
２００　ユーザデバイス
２０１　ＣＰＵ（Central processing Unit）
２０２　インタフェース
２０３　ＲＯＭ（Read-Only-Memory）
２０４　ＲＡＭ（Random Access Memory）
２０５　暗号処理部
２０６　メモリ部
２１０　セキュリティチップ
２２１　ユーザデバイス側制御部
２２２　外部メモリ部
２８０　デコーダ
３０１　システムホルダ
３０２　サービスプロバイダ
３０３　コンテンツクリエータ
３０４　ユーザデバイス
４１０　ユーザデバイス
４１１　セキュリティチップ
４２１　記憶手段
４２２　ストレージメディア
＊４３０　ユーザデバイス
４５０　サポートセンタ
４７０　ユーザデバイス
４７１　ストレージメディア
４７２　ユーザデバイス
４７５　サポートセンタ
５０１　ＣＰＵ（Central processing Unit）
５０２　ＲＯＭ（Read-Only-Memory）
５０３　ＲＡＭ（Random Access Memory）
５０４　ＨＤＤ
５０５　入力部
５０６　出力部
５０７　通信部
５０８　ドライブ
５０９　リムーバブル記録媒体
５１０　バス
５１１　入出力インタフェース
５１２　セキュリティチップ
６０１　ＣＰＵ(Central processing Unit)
６０２　ＲＯＭ（Read-Only-Memory）
６０３　ＲＡＭ（Random Access Memory）
６０４　ＨＤＤ
６０５　暗号処理手段
６０６　ドライブ
６０７　リムーバブル記録媒体
６０８，６０９　通信部
６１０　バス
＊

【図１】



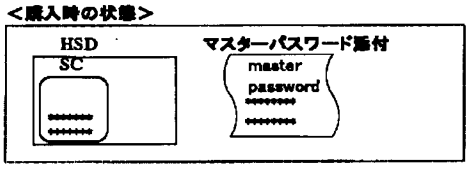
【図２】

Version		
V-1	version	証明書のフォーマットのバージョン
	serialNumber	証明書発行者によって割り当てられる証明書番号
	signature	証明書の署名アルゴリズム
	issuer	証明書発行者名(Distinguished Name形式)
	validity notBefore notAfter	証明書の有効期限 開始日時 終了日時
	subject	証明書所有者名
	subjectPublicKeyInfo algorithm subjectPublickey	証明書所有者の公開鍵情報 鍵のアルゴリズム 鍵

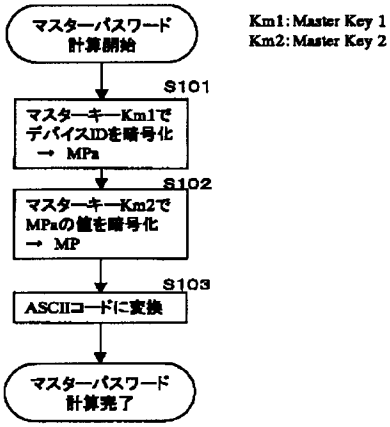
【図３】

V-3	authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	署名検証に用いる証明書発行者の鍵識別子 鍵識別子 機関証明書発行者名(General Name形式) 機関証明書シリアルナンバ
	subjectKeyIdentifier keyIdentifier	複数の鍵の中から目的の鍵を明確に識別
	key usage (0)digitalSignature (1)nonRepudiation (2)keyEncipherment (3)dataEncipherment (4)keyAgreement (5)keyCertSign (6)cRLSign	鍵の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配送用 (5)認証の署名確認用 (6)失効リストの署名確認用
	privateKeyUsagePeriod notBefore notAfter	証明書中の公開鍵に対応する秘密鍵の有効期限
	certificatePolicies policyIdentifier policyQualifiers	証明書発行者が承認した証明書ポリシー ポリシーID(ISO/IEC9834-1準拠) 認証基準
	policyMappings IssuerDomainPolicy subjectDomainPolicy	認証パス中のポリシーの関係を制限 （CA証明書にのみ必要）

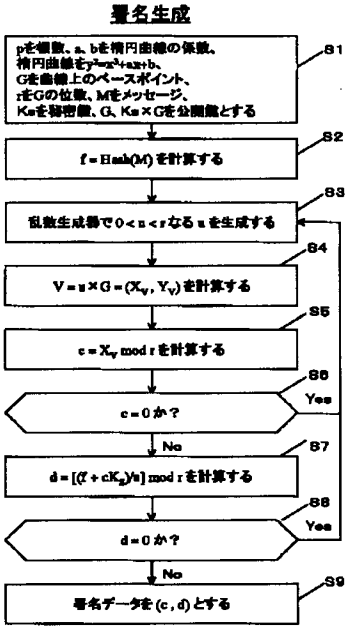
【図１２】



【図１４】



【図１９】

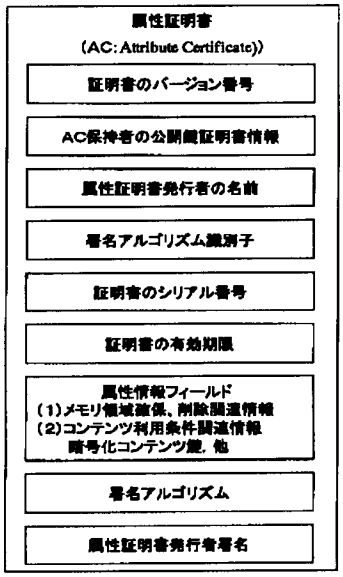


署名生成(IEEE P1363/D13)

【図４】

V-3	subjectAltName	証明書所有者の別名（GN形式）
	issuerAltName	証明書発行者の別名（GN形式）
	subjectDirectoryAttributes	証明書所有者のために必要とされるディレクトリの属性
	basicConstraints cA pathLenConstraint	証明対象の公開鍵が認証局の署名用か、証明書所有者のものかを区別
	nameConstraints permittedSubtrees base minimum maximum ExcludedSubtrees	発行者が発行する証明書の名前を制限
	policyConstraints requireExplicitPolicy inhibitPolicyMapping	認証パス中のポリシーの関係を制限
	cRLDistributionPoints	証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述
	signatureAlgorithm	証明書への署名付けに用いるアルゴリズム
	signatureValue	証明書発行者の秘密鍵による署名

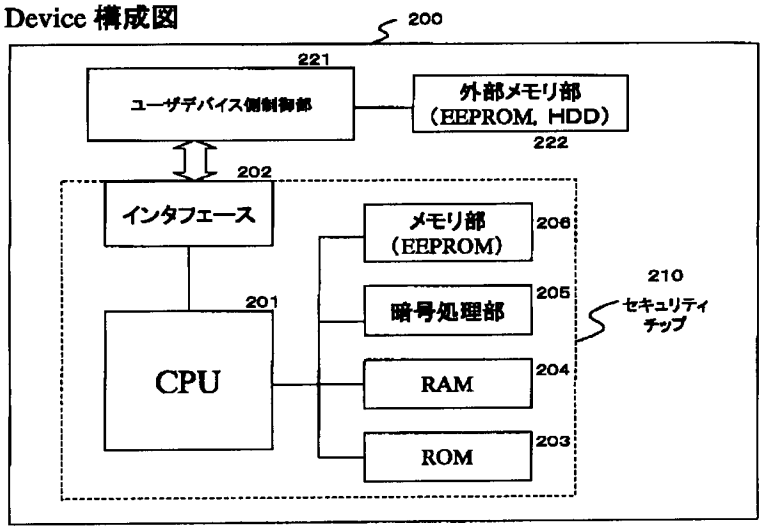
【図５】



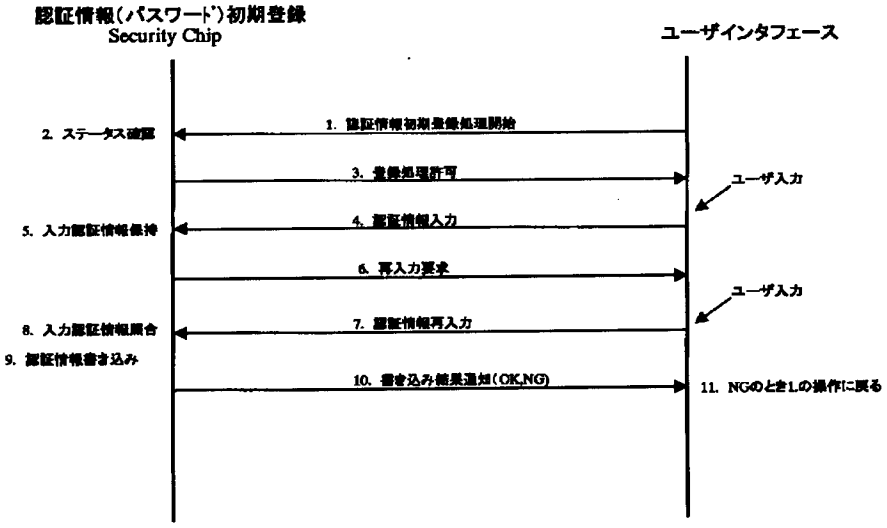
【図７】

データ種別	データ内容
公開鍵証明書	・ルート認証局公開鍵証明書 ・サービスプロバイダ公開鍵証明書 ・サポートセンタ公開鍵証明書
属性証明書	・アプリケーション（コンテンツ）利用管理用属性証明書 ・SP用メモリ領域管理用属性証明書
鍵データ	・公開鍵、秘密鍵ペア ・ストレージ鍵 （デバイス対応ストレージ鍵：グローバル共通鍵） （サービスプロバイダ対応ストレージ鍵） ・乱数生成用鍵、・相互認証用鍵
識別情報	・デバイスID ・サービスプロバイダID ・ユーザID ・アプリケーションID
その他	・認証情報 ・乱数シード（Seed） ・コンテンツ利用回数情報

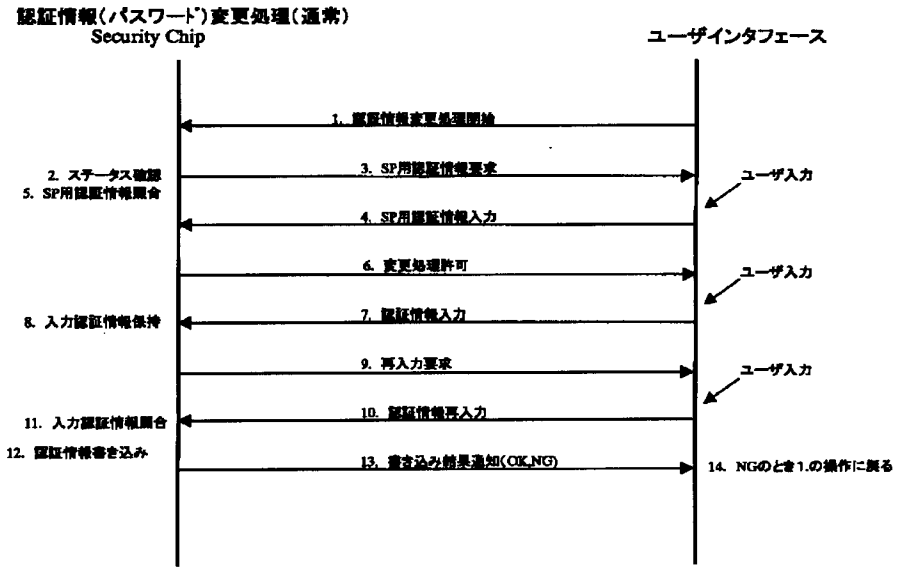
【図６】


Device 構成図
200
221
ユーザデバイス側制御部
外部メモリ部
(EEPROM, HDD)
222
202
インタフェース
メモリ部
(EEPROM)
206
210
セキュリティ
チップ
201
暗号処理部
205
CPU
RAM
204
ROM
203

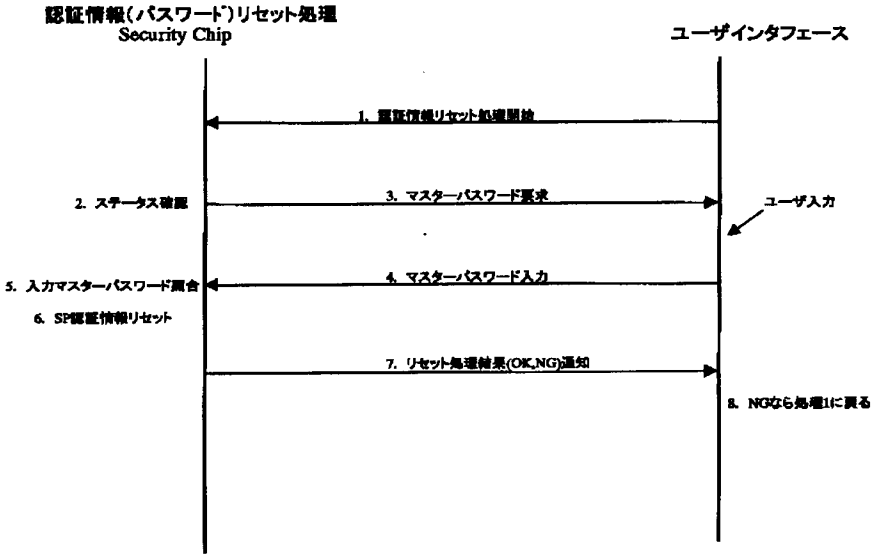
【図８】


認証情報(パスワード)初期登録
Security Chip
ユーザインタフェース
2. ステータス確認
1. 認証情報初期登録処理開始
3. 登録処理許可
ユーザ入力
5. 入力認証情報保持
4. 認証情報入力
6. 再入力要求
ユーザ入力
8. 入力認証情報照合
7. 認証情報再入力
9. 認証情報書き込み
10. 書き込み結果通知(OK,NG)
11. NGのとき1.の操作に戻る

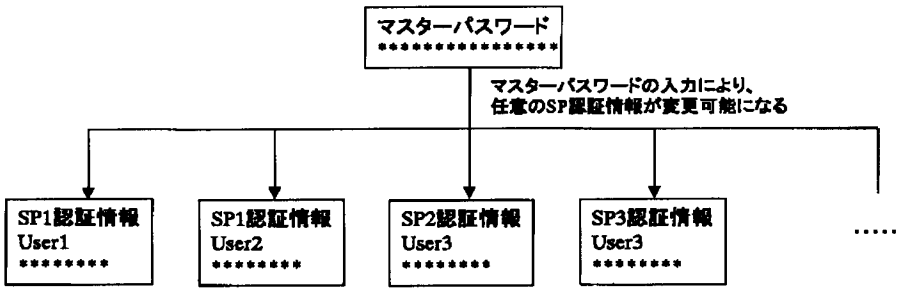
【図９】


認証情報(パスワード)変更処理(通常)
Security Chip
ユーザインタフェース
1. 認証情報変更処理開始
2. ステータス確認
3. SP用認証情報要求
ユーザ入力
5. SP用認証情報照合
4. SP用認証情報入力
6. 変更処理許可
ユーザ入力
8. 入力認証情報保持
7. 認証情報入力
9. 再入力要求
ユーザ入力
11. 入力認証情報照合
10. 認証情報再入力
12. 認証情報書き込み
13. 書き込み結果通知(OK,NG)
14. NGのとき1.の操作に戻る

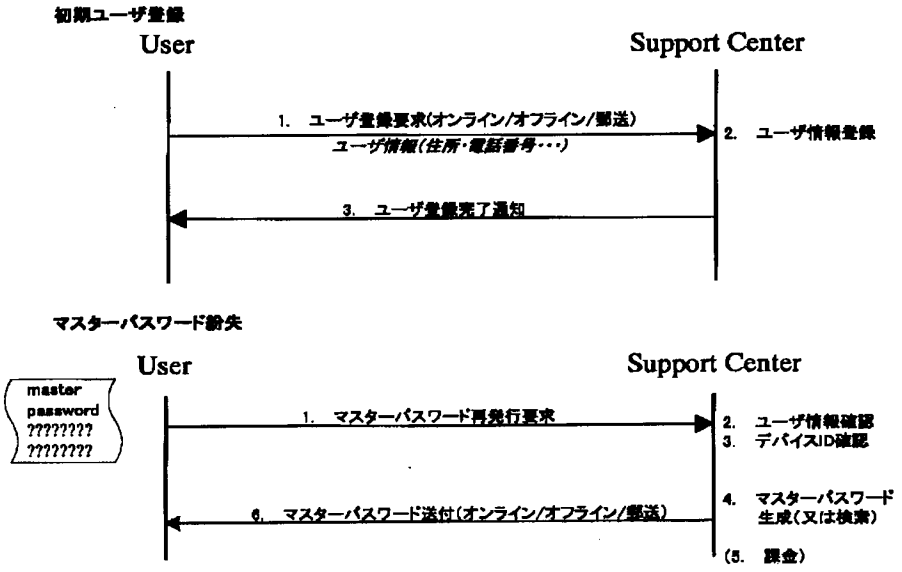
【図１０】


認証情報(パスワード)リセット処理
Security Chip
ユーザインタフェース
1. 認証情報リセット処理開始
2. ステータス確認
3. マスターパスワード要求
ユーザ入力
5. 入力マスターパスワード照合
4. マスターパスワード入力
6. SP認証情報リセット
7. リセット処理結果(OK,NG)通知
8. NGなら処理1に戻る

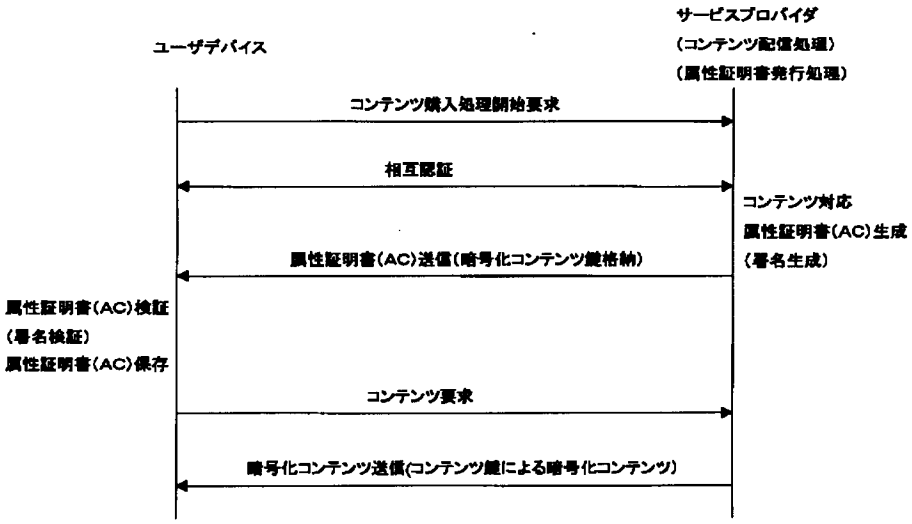
【図１１】


マスターパスワード
****
マスターパスワードの入力により、
任意のSP認証情報が変更可能になる
SP1認証情報
User1
****
SP1認証情報
User2
****
SP2認証情報
User3
****
SP3認証情報
User3
****
.....

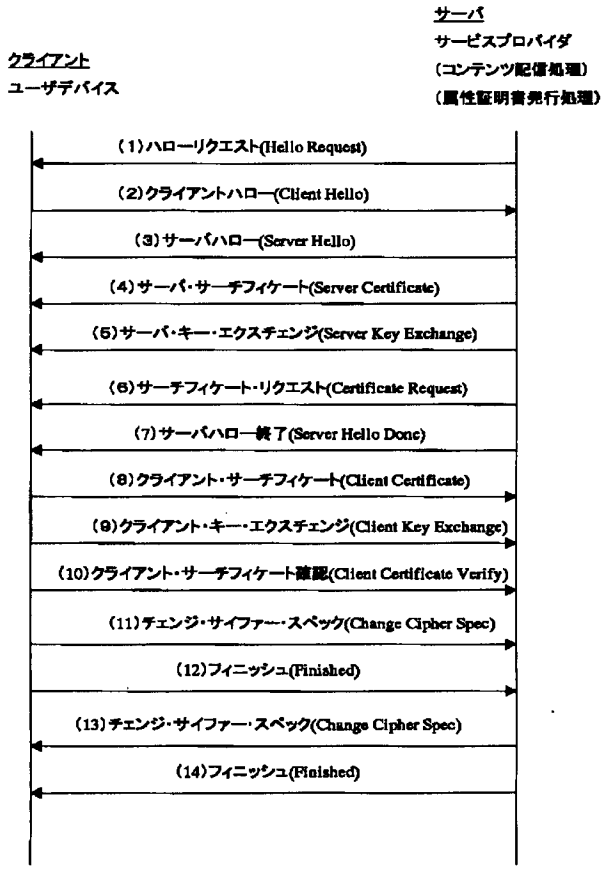
【図１３】


初期ユーザ登録
User
Support Center
1. ユーザ登録要求(オンライン/オフライン/郵送)
ユーザ情報(住所・電話番号・・・)
2. ユーザ情報登録
3. ユーザ登録完了通知
マスターパスワード紛失
User
Support Center
master
password
????????
????????
1. マスターパスワード再発行要求
2. ユーザ情報確認
3. デバイスID確認
4. マスターパスワード
生成(又は検索)
6. マスターパスワード送付(オンライン/オフライン/郵送)
(5. 課金)

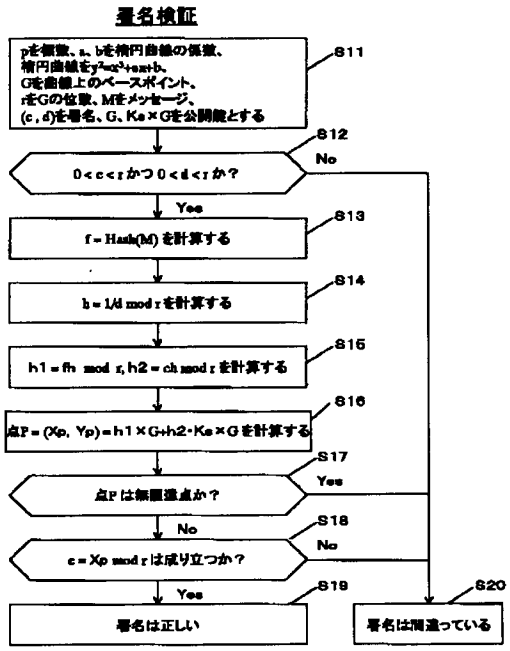
【図１５】



【図１６】

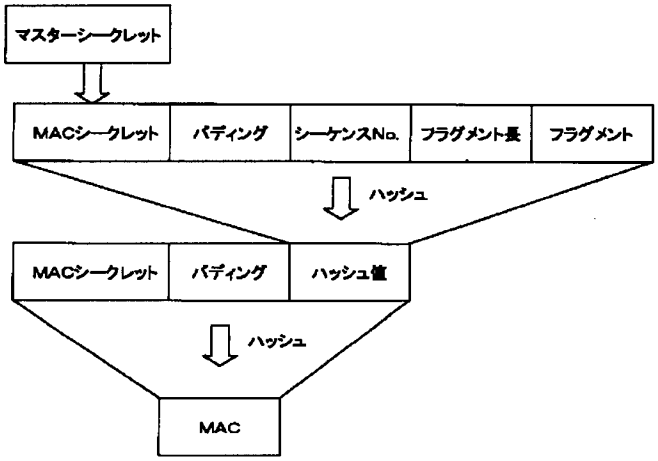


【図２０】

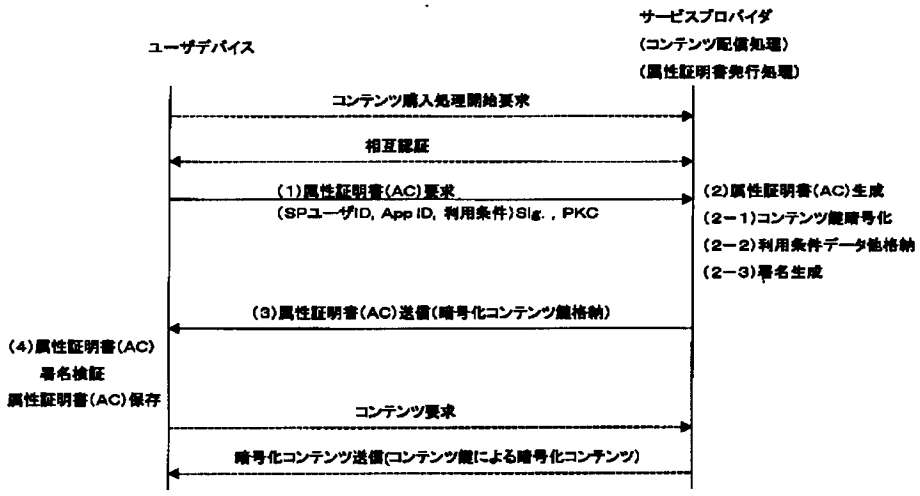


署名検証(IEEE P1363/D13)

【図１７】

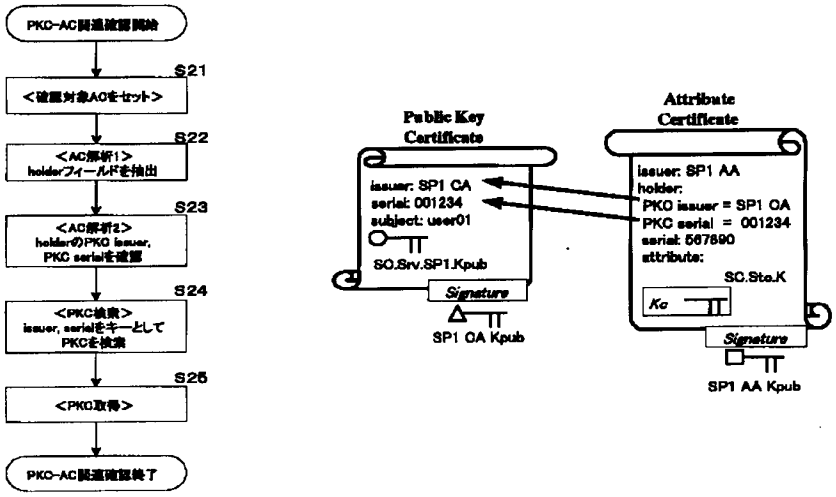

マスターシークレット
MACシークレット
パディング
シーケンスNo.
フラグメント長
フラグメント
ハッシュ
MACシークレット
パディング
ハッシュ値
ハッシュ
MAC

【図１８】

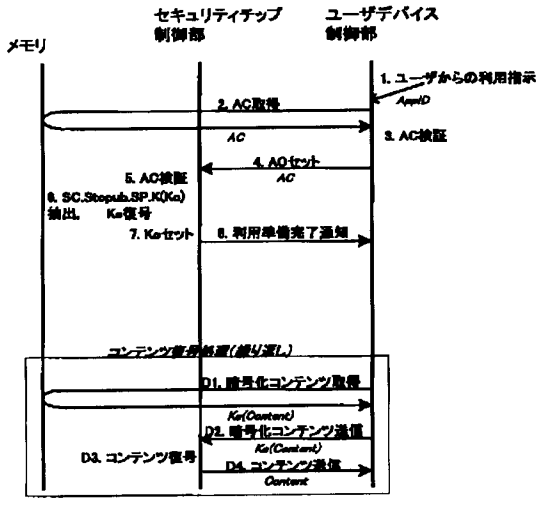

ユーザデバイス
サービスプロバイダ
(コンテンツ配信処理)
(属性証明書発行処理)
コンテンツ購入処理開始要求
相互認証
(1)属性証明書(AC)要求
(SPユーザID, App ID, 利用条件)Sig. , PKC
(2)属性証明書(AC)生成
(2−1)コンテンツ鍵暗号化
(2−2)利用条件データ他格納
(2−3)署名生成
(3)属性証明書(AC)送信(暗号化コンテンツ鍵格納)
(4)属性証明書(AC)
署名検証
属性証明書(AC)保存
コンテンツ要求
暗号化コンテンツ送信(コンテンツ鍵による暗号化コンテンツ)

【図２１】

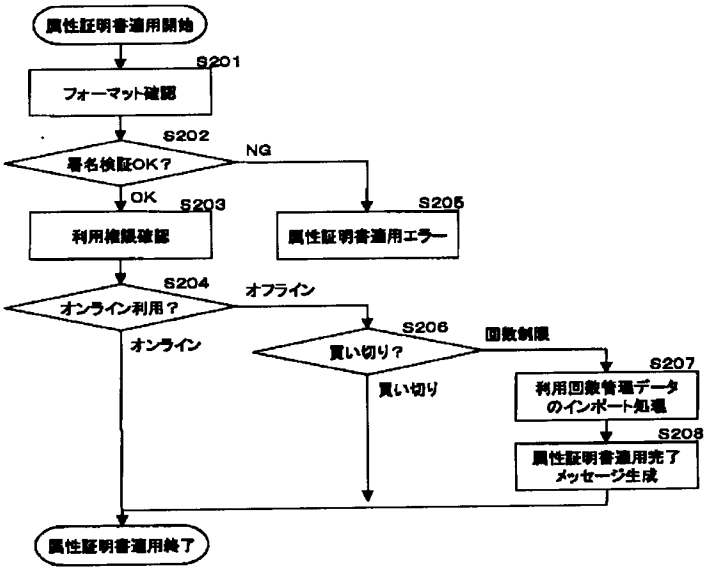
PKCとACの関連づけ



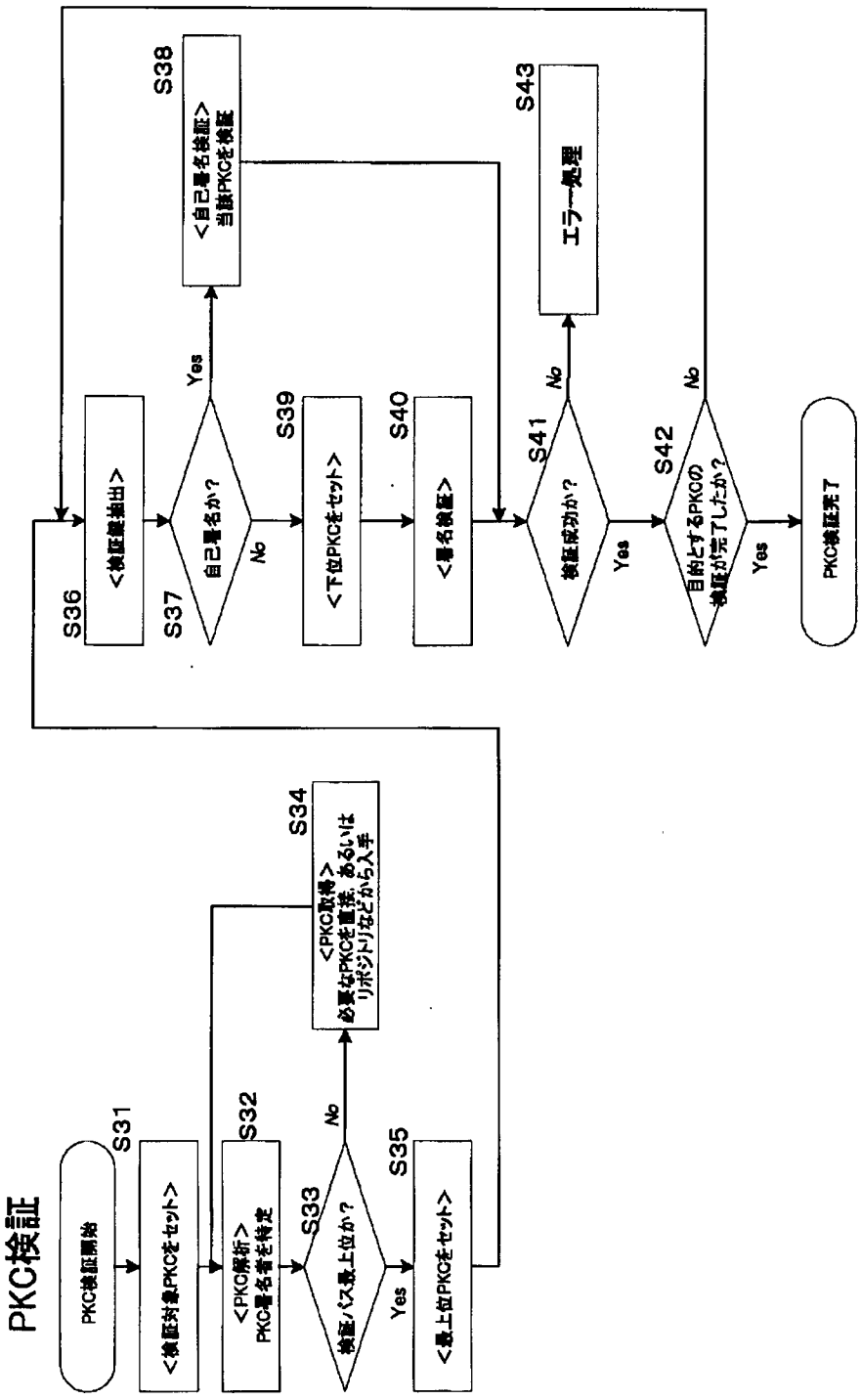
【図２５】



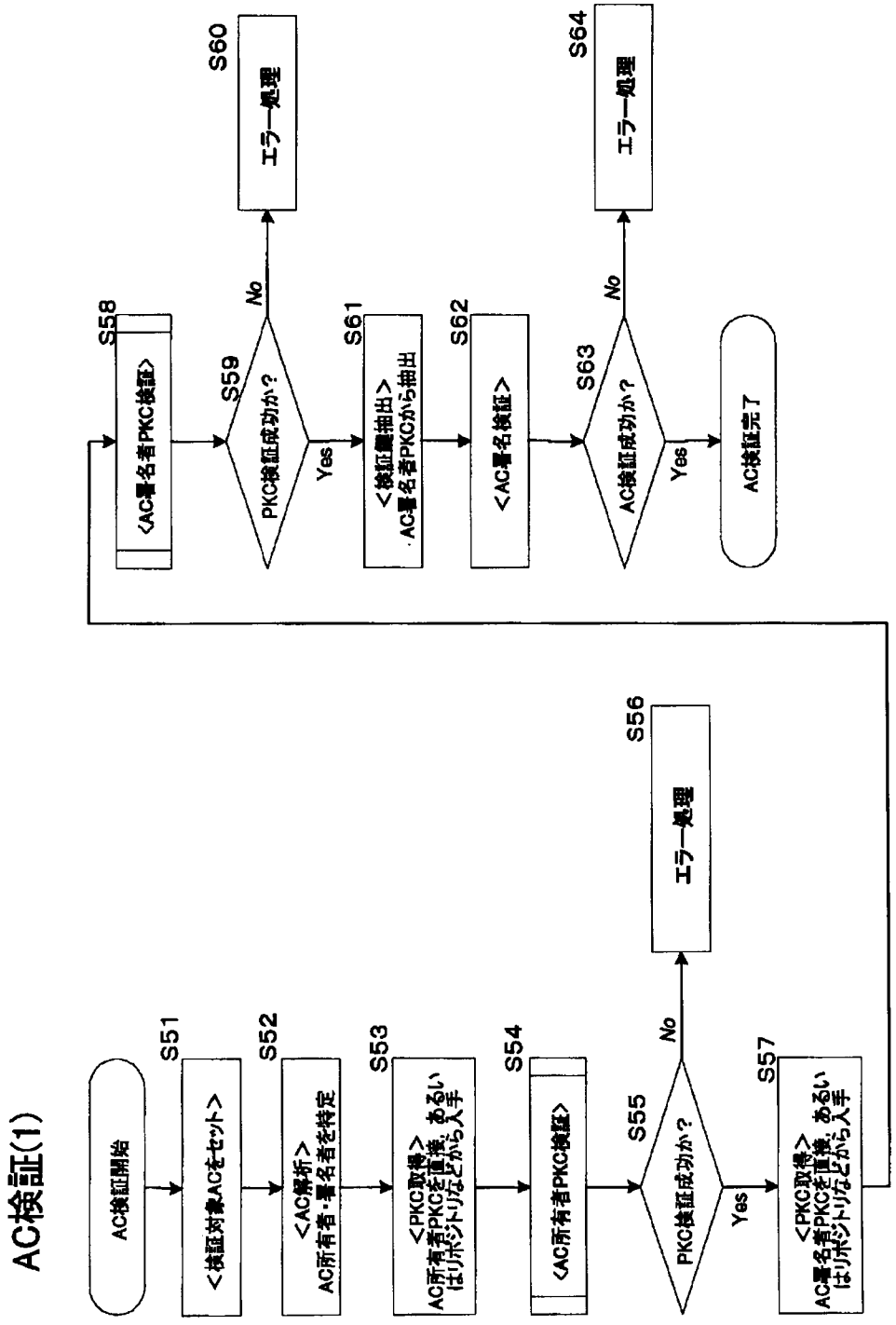
【図３３】



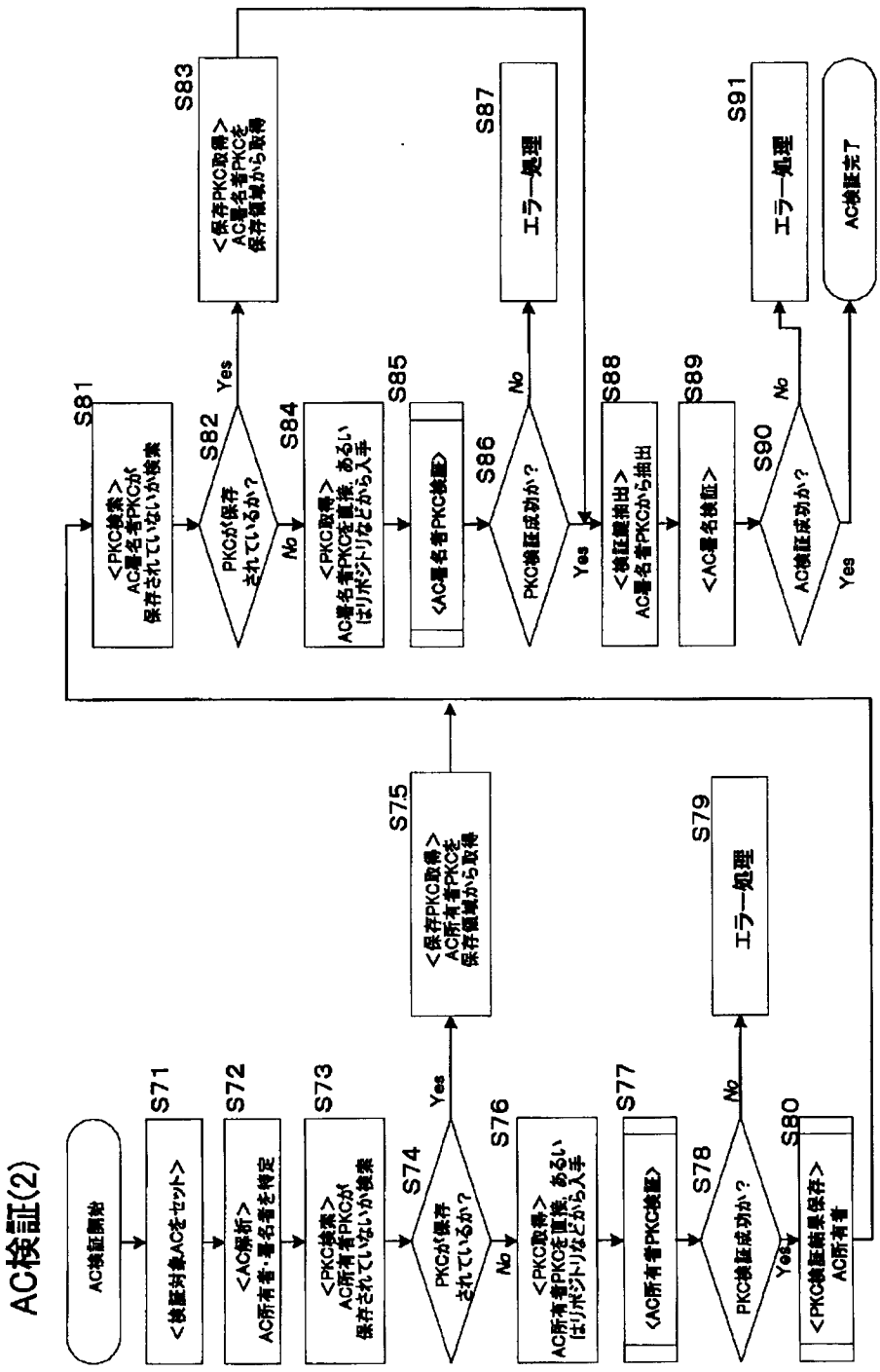
【図２２】


PKC検証
PKC検証開始
S31
<検証対象PKCをセット>
S32
<PKC解析>
PKC署名者を特定
S33
検証パス最上位か？
No
Yes
S34
<PKC取得>
必要なPKCを直接、あるいは
リポジトリなどから入手
S35
<最上位PKCをセット>
S36
<検証鍵抽出>
S37
自己署名か？
Yes
No
S38
<自己署名検証>
当該PKCを検証
S39
<下位PKCをセット>
S40
<署名検証>
S41
検証成功か？
No
Yes
S43
エラー処理
S42
目的とするPKCの
検証が完了したか？
No
Yes
PKC検証完了

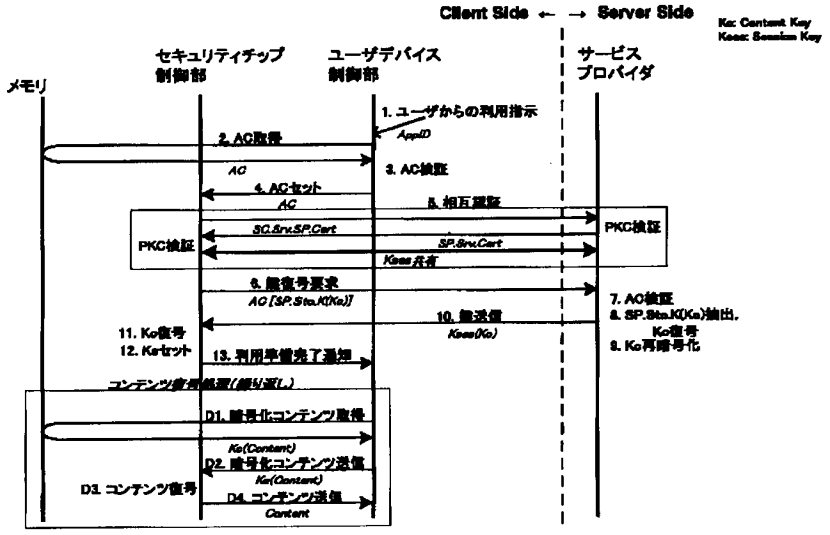
【図２３】


AC検証(1)
AC検証開始
S51
<検証対象ACをセット>
S52
<AC解析>
AC所有者・署名者を特定
S53
<PKC取得>
AC所有者PKCを直接、あるいはリポジトリなどから入手
S54
<AC所有者PKC検証>
S55
PKC検証成功か？
No
Yes
S56
エラー処理
S57
<PKC取得>
AC署名者PKCを直接、あるいはリポジトリなどから入手
S58
<AC署名者PKC検証>
S59
PKC検証成功か？
No
Yes
S60
エラー処理
S61
<検証鍵抽出>
AC署名者PKCから抽出
S62
<AC署名検証>
S63
AC検証成功か？
No
Yes
S64
エラー処理
AC検証完了

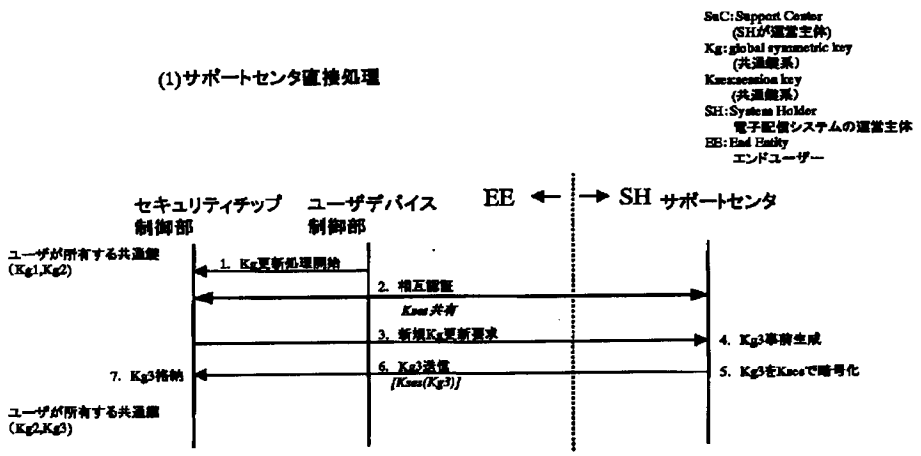
【図２４】


AC検証(2)
AC検証開始
S71
<検証対象ACをセット>
S72
<AC解析>
AC所有者・署名者を特定
S73
<PKC検索>
AC所有者PKCが
保存されていないか検索
S74
PKCが保存
されているか?
Yes
No
S75
<保存PKC取得>
AC所有者PKCを
保存領域から取得
S76
<PKC取得>
AC所有者PKCを直接、あるい
はリポジトリなどから入手
S77
<AC所有者PKC検証>
S78
PKC検証成功か?
No
Yes
S79
エラー処理
S80
<PKC検証結果保存>
AC所有者
S81
<PKC検索>
AC署名者PKCが
保存されていないか検索
S82
PKCが保存
されているか?
Yes
No
S83
<保存PKC取得>
AC署名者PKCを
保存領域から取得
S84
<PKC取得>
AC署名者PKCを直接、あるい
はリポジトリなどから入手
S85
<AC署名者PKC検証>
S86
PKC検証成功か?
No
Yes
S87
エラー処理
S88
<検証属性抽出>
AC署名者PKCから抽出
S89
<AC署名検証>
S90
AC検証成功か?
No
Yes
S91
エラー処理
AC検証完了

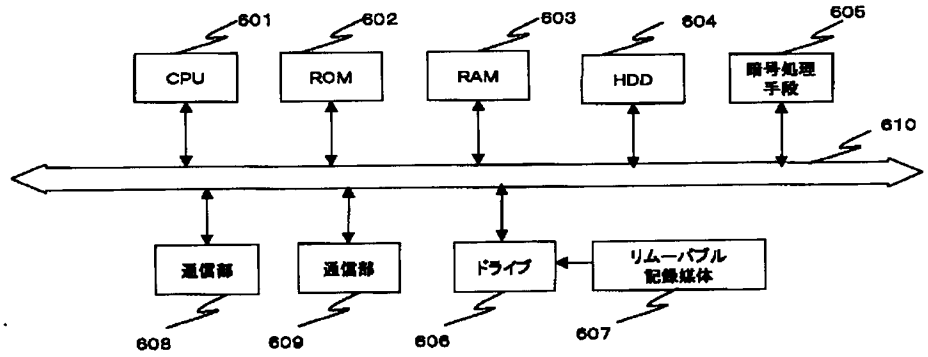
【図２６】


Client Side ← → Server Side
Kc: Content Key
Kcon: Session Key
メモリ
セキュリティチップ 制御部
ユーザデバイス 制御部
サービス プロバイダ
1. ユーザからの利用指示
AppID
2. AC取得
AC
3. AC検証
4. ACセット
AC
5. 相互認証
SC.Srv.SP.Cert
SP.Srv.Cert
Kcon共有
PKC検証
PKC検証
6. 鍵復号要求
AC [SP.Sto.K(Kc)]
7. AC検証
8. SP.Sto.K(Kc)抽出、Kc復号
9. Kc再暗号化
10. 鍵送信
Kcon(Kc)
11. Kc復号
12. Kcセット
13. 利用準備完了通知
コンテンツ復号処理(繰り返し)
D1. 暗号化コンテンツ取得
Kc(Content)
D2. 暗号化コンテンツ送信
Kc(Content)
D3. コンテンツ復号
D4. コンテンツ送信
Content

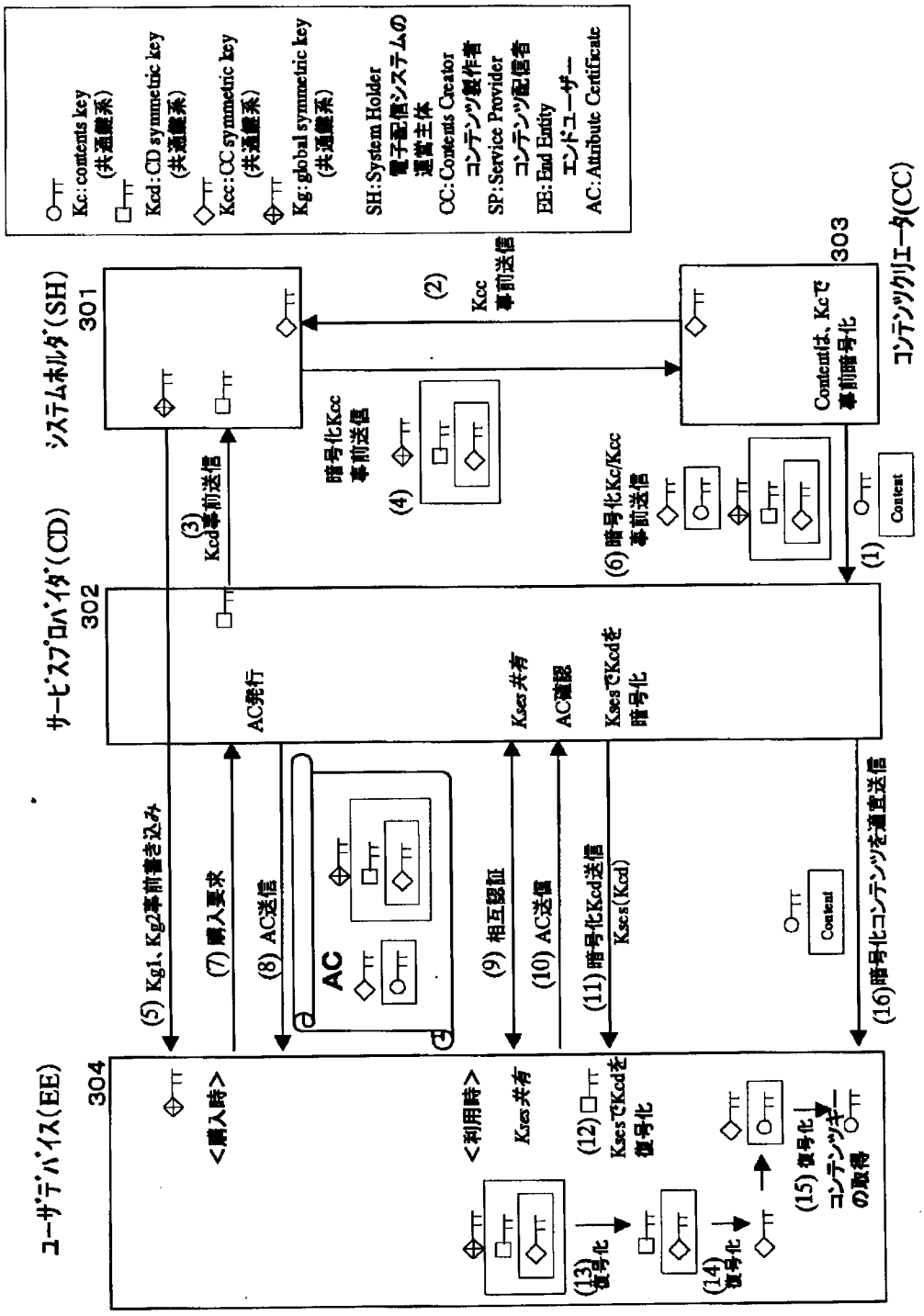
【図２８】


SuC: Support Center (SHが運営主体)
Kg: global symmetric key (共通鍵系)
Kseasession key (共通鍵系)
SH: System Holder 電子配信システムの運営主体
EE: End Entity エンドユーザー
(1)サポートセンタ直接処理
セキュリティチップ 制御部
ユーザデバイス 制御部
EE ← → SH サポートセンタ
ユーザが所有する共通鍵 (Kg1,Kg2)
1. Kg更新処理開始
2. 相互認証
Kseas共有
3. 新規Kg更新要求
4. Kg3事前生成
5. Kg3をKseasで暗号化
6. Kg3送信
[Kseas(Kg3)]
7. Kg3格納
ユーザが所有する共通鍵 (Kg2,Kg3)

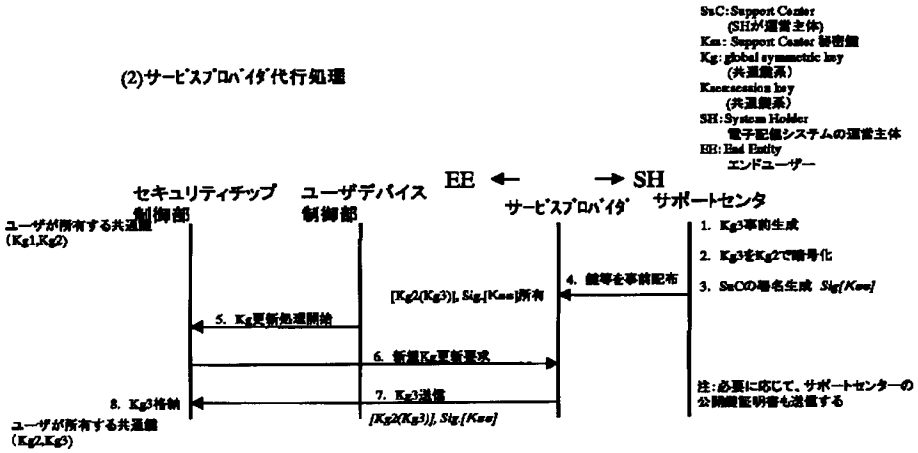
【図５５】


601
602
603
604
605
CPU
ROM
RAM
HDD
暗号処理手段
610
通信部
通信部
ドライブ
リムーバブル記録媒体
608
609
606
607

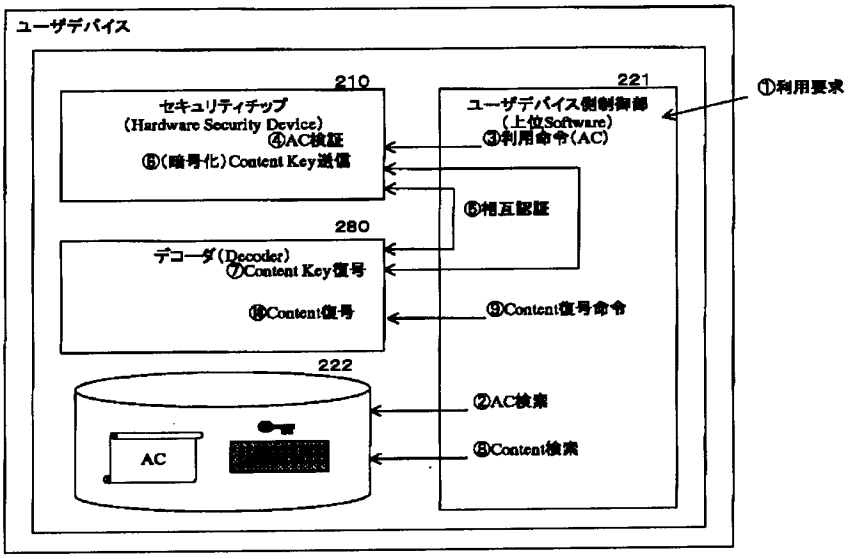
【図２７】


Kc: contents key (共通鍵系)
Kcd: CD symmetric key (共通鍵系)
Kcc: CC symmetric key (共通鍵系)
Kg: global symmetric key (共通鍵系)
SH: System Holder 電子配信システムの運営主体
CC: Contents Creator コンテンツ製作者
SP: Service Provider コンテンツ配信者
EE: End Entity エンドユーザー
AC: Attribute Certificate
システムホルダ(SH) 301
サービスプロバイダ(CD) 302
コンテンツクリエータ(CC) 303
ユーザデバイス(EE) 304
(2) Kcc 事前送信
暗号化Kcc 事前送信
(3) Kcd事前送信
(4)
Contentは、Kcで事前暗号化
(6) 暗号化Kc/Kcc 事前送信
(1) Content
AC発行
(5) Kg1、Kg2事前書き込み
(7) 購入要求
(8) AC送信
AC
Ksesで Kcdを暗号化
AC確認
Kses共有
(9) 相互認証
(10) AC送信
(11) 暗号化Kcd送信
Kses(Kcd)
Content
(16)暗号化コンテンツを通常送信
<購入時>
<利用時>
Kses共有
(12) Ksesで Kcdを復号化
(13) 復号化
(14) 復号化
(15) 復号化 コンテンツキーの取得

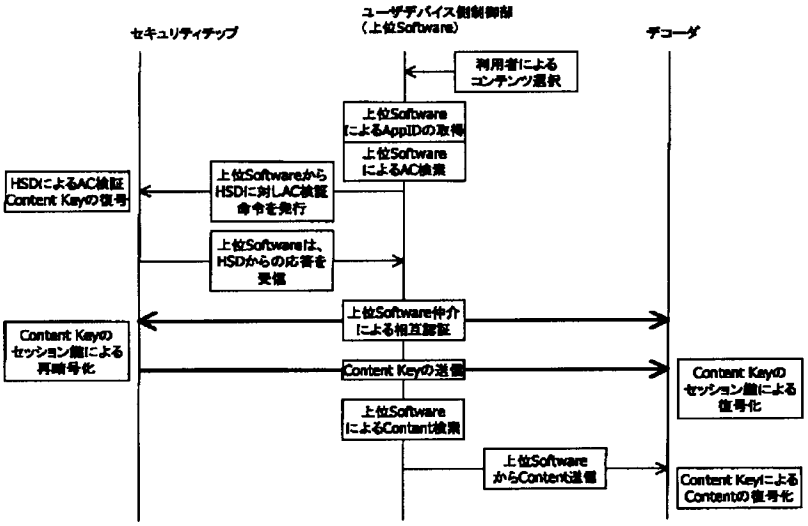
【図２９】


SnC:Support Center
(SHが運営主体)
Km: Support Center 秘密鍵
Kg: global symmetric key
(共通鍵系)
Kmsession key
(共通鍵系)
SH:System Holder
電子配信システムの運営主体
EE: End Entity
エンドユーザー
(2)サービスプロバイダ代行処理
EE
SH
セキュリティチップ制御部
ユーザデバイス制御部
サービスプロバイダ
サポートセンタ
ユーザが所有する共通鍵
(Kg1,Kg2)
1. Kg3事前生成
2. Kg3をKg2で暗号化
3. SnCの署名生成 Sig[Kmn]
4. 鍵等を事前配布
[Kg2(Kg3)], Sig.[Kmn]所有
5. Kg更新処理開始
6. 新規Kg更新要求
7. Kg3送信
[Kg2(Kg3)], Sig.[Kmn]
8. Kg3格納
ユーザが所有する共通鍵
(Kg2,Kg3)
注:必要に応じて、サポートセンターの
公開鍵証明書も送信する

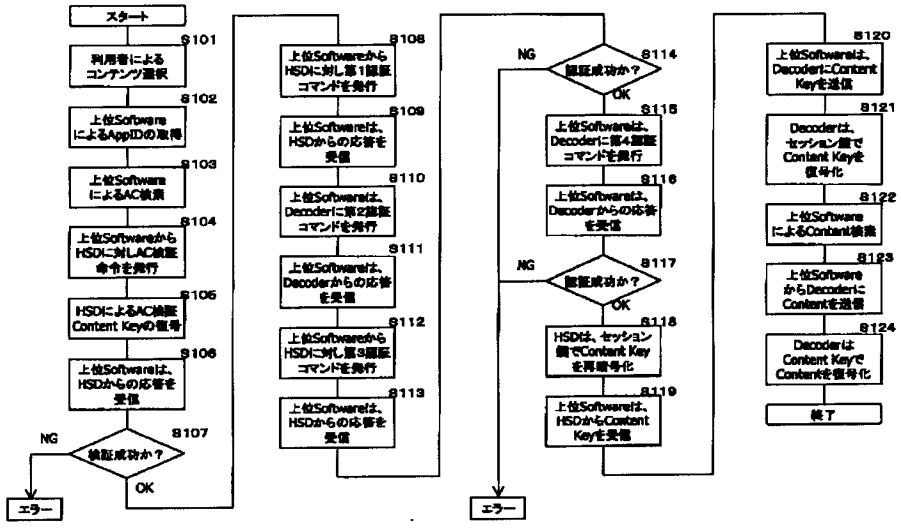
【図３０】


ユーザデバイス
210
セキュリティチップ
(Hardware Security Device)
④AC検証
⑥(暗号化)Content Key送信
221
ユーザデバイス側制御部
(上位Software)
①利用要求
③利用命令(AC)
⑤相互認証
280
デコーダ(Decoder)
⑦Content Key復号
⑧Content復号
⑨Content復号命令
222
AC
②AC検索
⑤Content検索

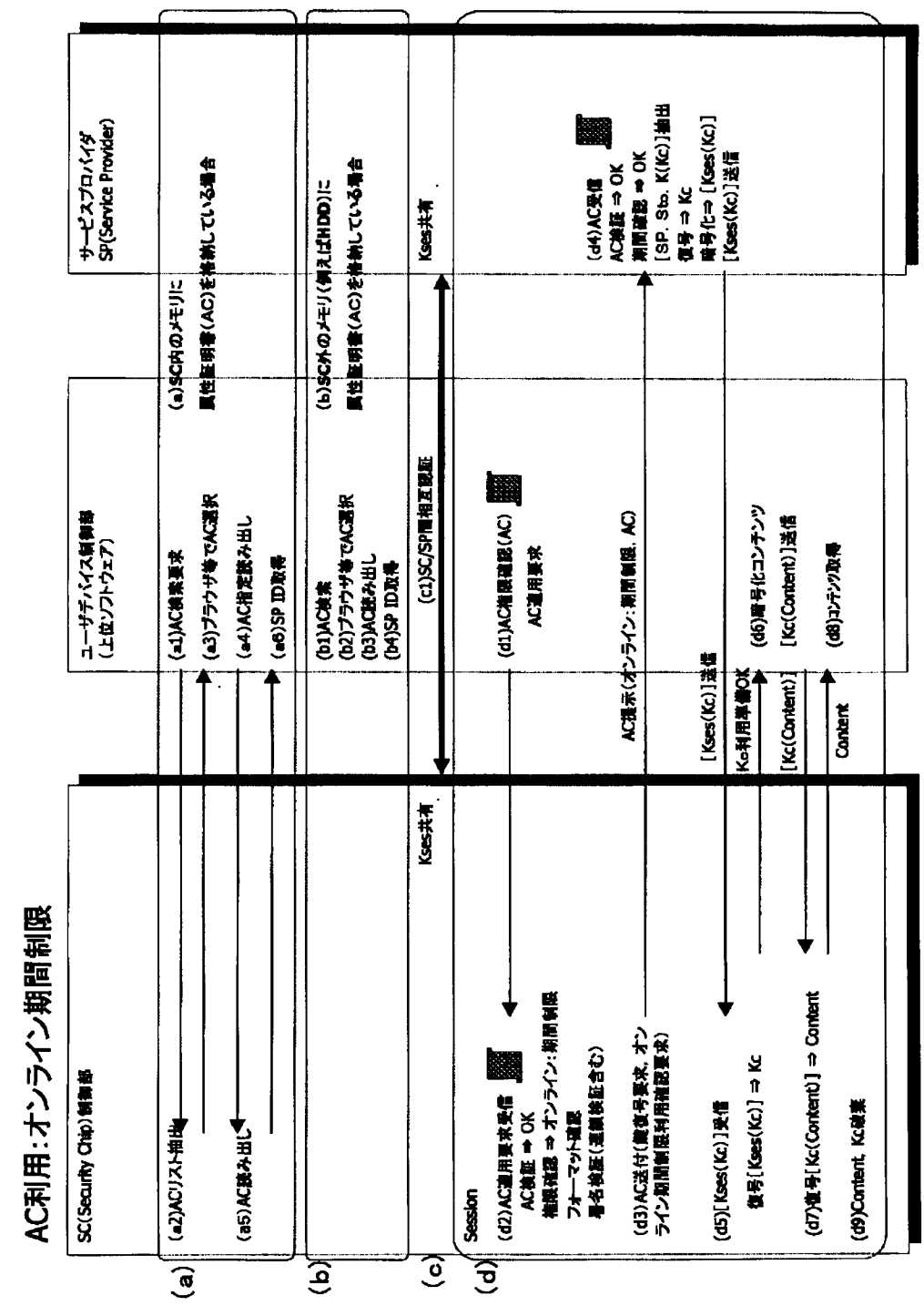
【図３１】


セキュリティチップ
ユーザデバイス側制御部
（上位Software）
デコーダ
利用者による
コンテンツ選択
上位Software
によるAppIDの取得
上位Software
によるAC検索
HSDによるAC検証
Content Keyの復号
上位Softwareから
HSDに対しAC検証
命令を発行
上位Softwareは、
HSDからの応答を
受信
上位Software仲介
による相互認証
Content Keyの
セッション鍵による
再暗号化
Content Keyの送信
Content Keyの
セッション鍵による
復号化
上位Software
によるContent検索
上位Software
からContent送信
Content Keyによる
Contentの復号化

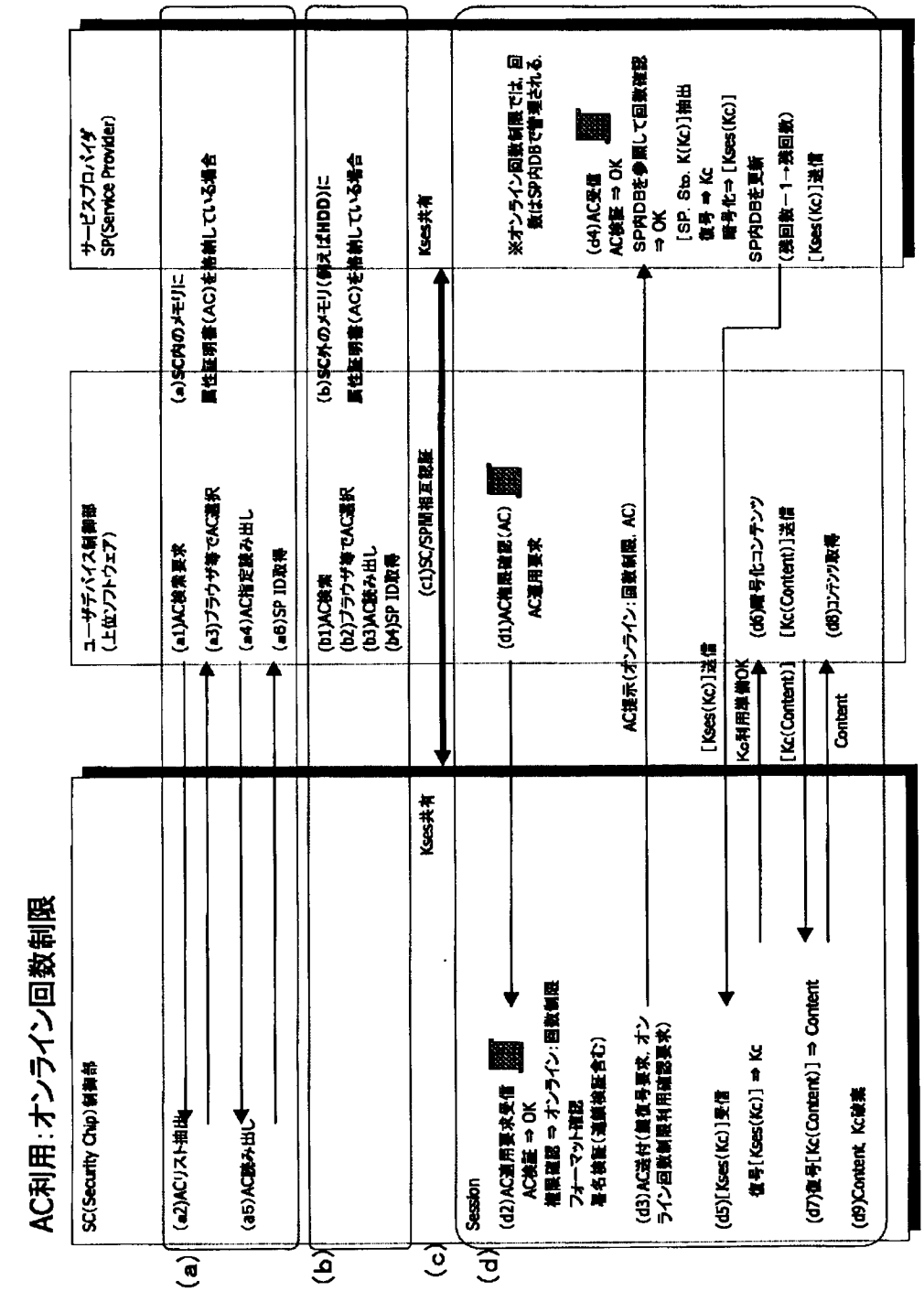
【図３２】


スタート
S101
利用者による
コンテンツ選択
S102
上位Software
によるAppIDの取得
S103
上位Software
によるAC検索
S104
上位Softwareから
HSDに対しAC検証
命令を発行
S105
HSDによるAC検証
Content Keyの復号
S106
上位Softwareは、
HSDからの応答を
受信
S107
NG
検証成功か？
OK
エラー
S108
上位Softwareから
HSDに対し第1認証
コマンドを発行
S109
上位Softwareは、
HSDからの応答を
受信
S110
上位Softwareは、
Decoderに第2認証
コマンドを発行
S111
上位Softwareは、
Decoderからの応答
を受信
S112
上位Softwareから
HSDに対し第3認証
コマンドを発行
S113
上位Softwareは、
HSDからの応答を
受信
S114
NG
認証成功か？
OK
エラー
S115
上位Softwareは、
Decoderに第4認証
コマンドを発行
S116
上位Softwareは、
Decoderからの応答
を受信
S117
NG
認証成功か？
OK
S118
HSDは、セッション
鍵でContent Key
を再暗号化
S119
上位Softwareは、
HSDからContent
Keyを受信
S120
上位Softwareは、
DecoderにContent
Keyを送信
S121
Decoderは、
セッション鍵で
Content Keyを
復号化
S122
上位Software
によるContent検索
S123
上位Software
からDecoderに
Contentを送信
S124
Decoderは
Content Keyで
Contentを復号化
終了

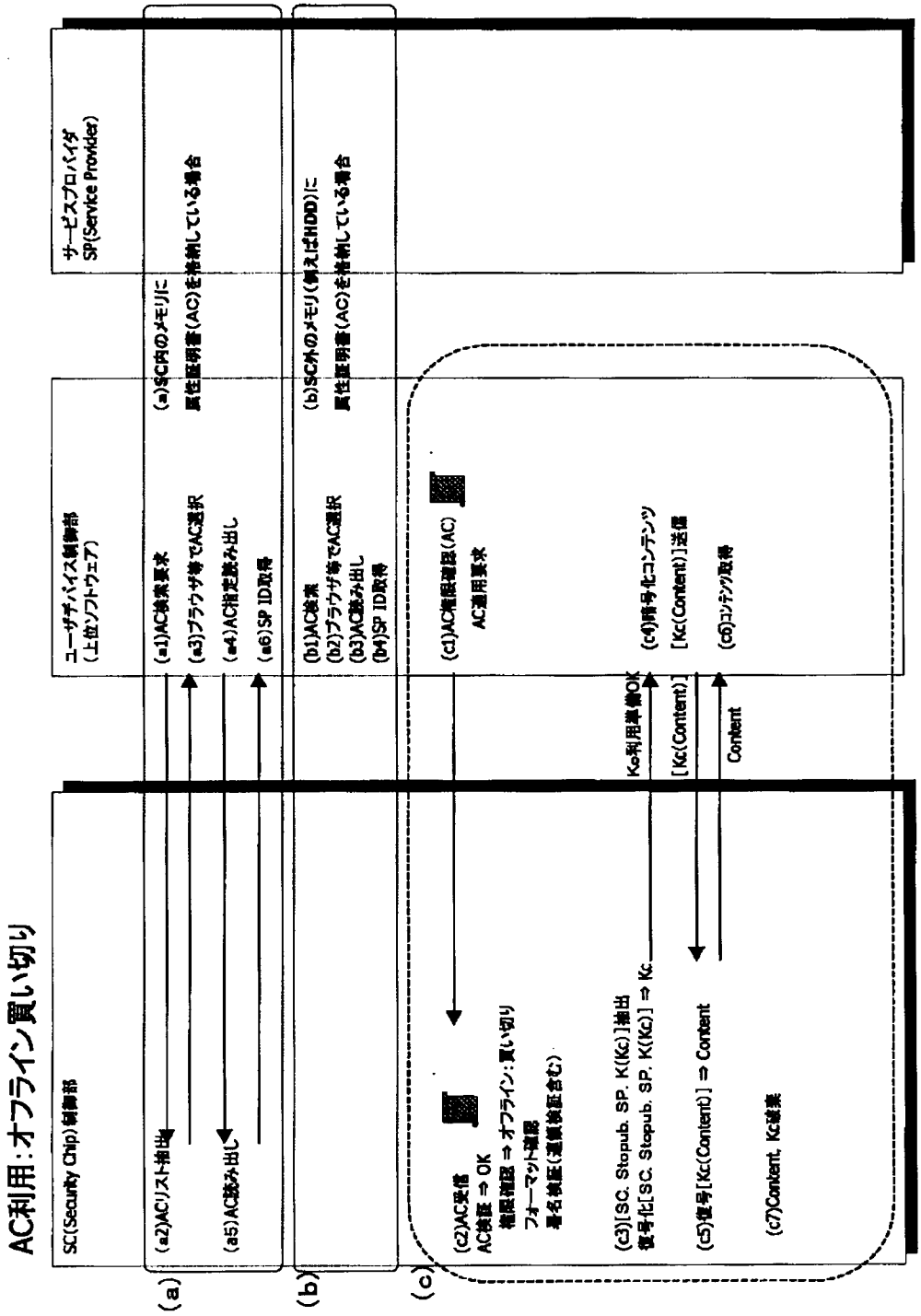
【図３４】


AC利用:オンライン期間制限
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
AC選用要求
(d2)AC選用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:期間制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(復号要求, オンライン期間制限利用権限要求)
AC提示(オンライン:期間制限 AC)
(d4)AC受信
AC検証 ⇒ OK
期間確認 ⇒ OK
[SP. Sto. K(Kc)]抽出
復号 ⇒ Kc
暗号化⇒ [Kses(Kc)]
[Kses(Kc)]送信
[Kses(Kc)]受信
復号[Kses(Kc)] ⇒ Kc
Kc利用準備OK
(d5)
(d6)暗号化コンテンツ
[Kc(Content)]送信
[Kc(Content)]
(d7)復号[Kc(Content)] ⇒ Content
Content
(d8)コンテンツ取得
(d9)Content Kc破棄

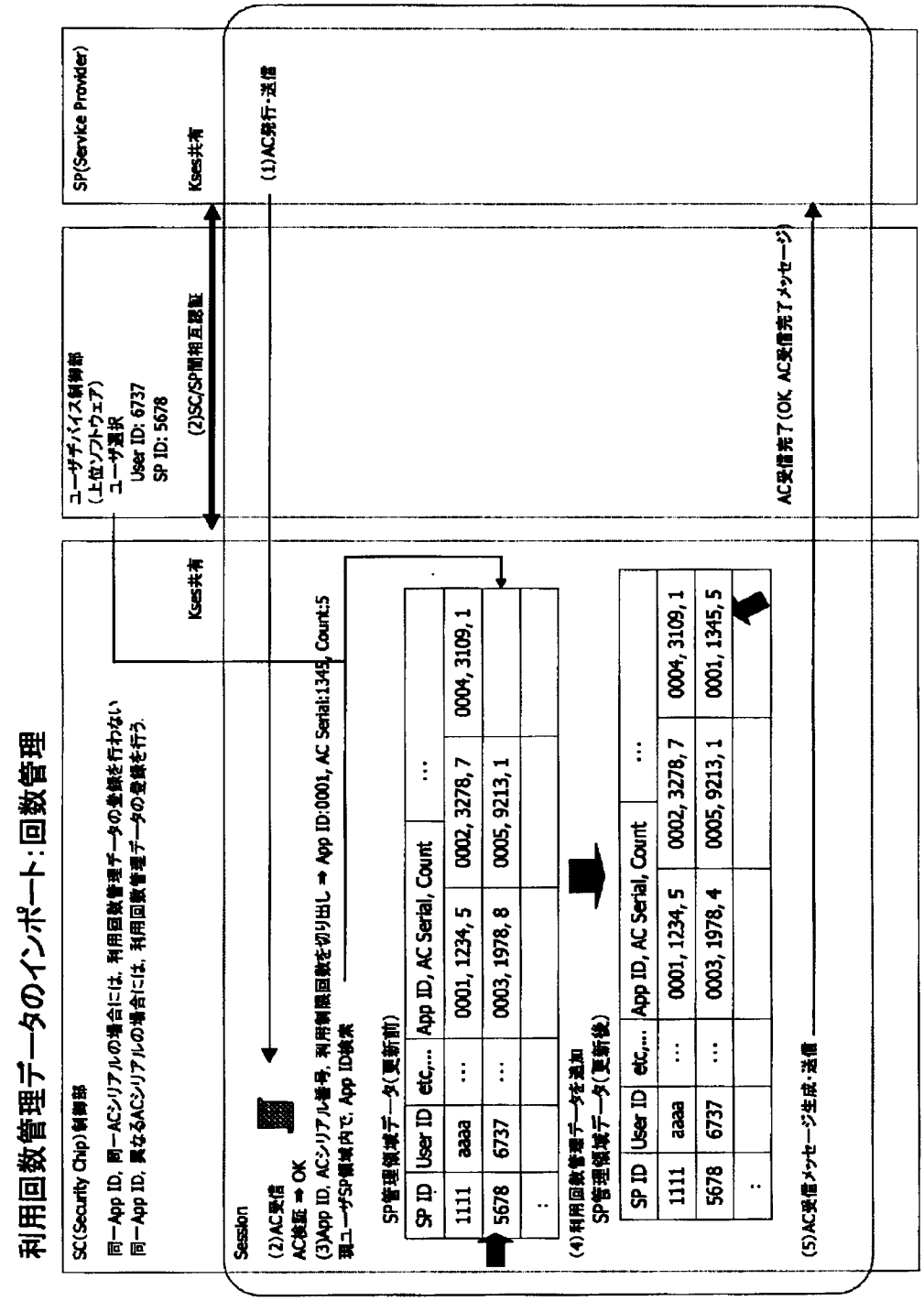
【図３５】


AC利用：オンライン回数制限
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
AC選用要求
(d2)AC選用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン：回数制限
フォーマット確認
署名検証(連鎖検証含む)
※オンライン回数制限では、回数はSP内DBで管理される。
(d4)AC受信
AC検証 ⇒ OK
SP内DBを参照して回数確認
⇒ OK
[SP. Sbo. K(Kc)]抽出
復号 ⇒ Kc
暗号化⇒ [Kses(Kc)]
SP内DBを更新
(残回数－1→残回数)
[Kses(Kc)]送信
(d3)AC送付(属性号要求、オンライン回数制限利用確認要求)
AC提示(オンライン：回数制限、AC)
[Kses(Kc)]送信
(d5)[Kses(Kc)]受信
復号[Kses(Kc)] ⇒ Kc
Kc利用準備OK
(d6)暗号化コンテンツ
[Kc(Content)]
[Kc(Content)]送信
(d7)復号[Kc(Content)] ⇒ Content
Content
(d8)コンテンツ取得
(d9)Content、Kc破棄

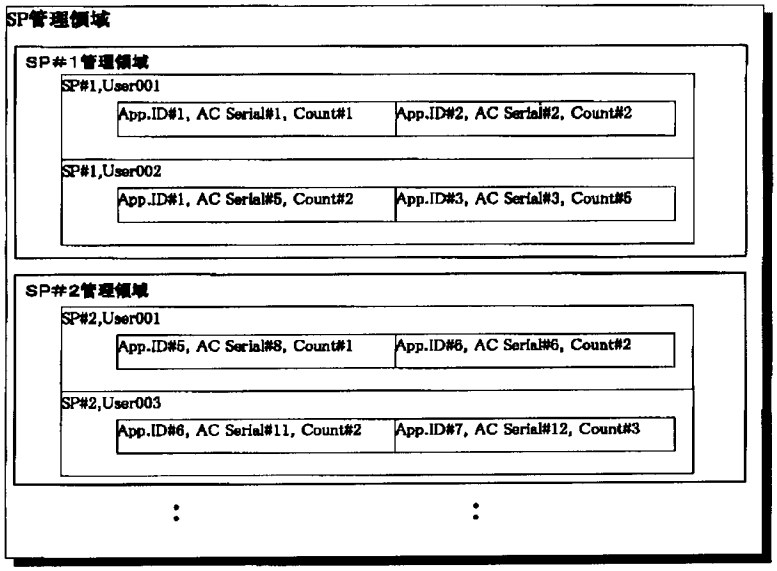
【図３６】


AC利用：オフライン買い切り
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)AC情報確認(AC)
AC適用要求
(c2)AC受信
AC検証 ⇒ OK
有効期限 ⇒ オフライン：買い切り
フォーマット確認
署名検証(運営検証含む)
(c3)[SC. Stopub. SP. K(Kc)]抽出
復号化[SC. Stopub. SP. K(Kc)] ⇒ Kc
Kc利用準備OK
(c4)暗号化コンテンツ
[Kc(Content)]送信
(c5)復号[Kc(Content)] ⇒ Content
(c6)コンテンツ取得
Content
(c7)Content, Kc破棄

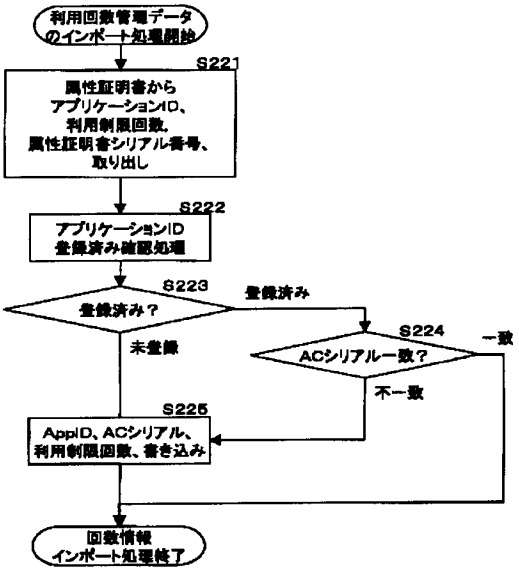
【図３７】


利用回数管理データのインポート：回数管理
SC(Security Chip)制御部
同一App ID, 同一ACシリアルの場合には，利用回数管理データの登録を行わない
同一App ID, 異なるACシリアルの場合には，利用回数管理データの登録を行う．
ユーザデバイス制御部
(上位ソフトウェア)
ユーザ選択
User ID: 6737
SP ID: 5678
SP(Service Provider)
(2)SC/SP間相互認証
Kses共有
Kses共有
(1)AC発行・送信
Session
(2)AC受信
AC検証 ⇒ OK
(3)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0001, AC Serial:1345, Count:5
現ユーザSP領域内で, App ID検索
SP管理領域データ(更新前)
SP ID
User ID
etc,...
App ID, AC Serial, Count
...
1111 aaaa ... 0001, 1234, 5 0002, 3278, 7 0004, 3109, 1
5678 6737 ... 0003, 1978, 8 0005, 9213, 1
(4)利用回数管理データを追加
SP管理領域データ(更新後)
SP ID
User ID
etc,...
App ID, AC Serial, Count
...
1111 aaaa ... 0001, 1234, 5 0002, 3278, 7 0004, 3109, 1
5678 6737 ... 0003, 1978, 4 0005, 9213, 1 0001, 1345, 5
AC受信完了(OK, AC受信完了メッセージ)
(5)AC受信メッセージ生成・送信

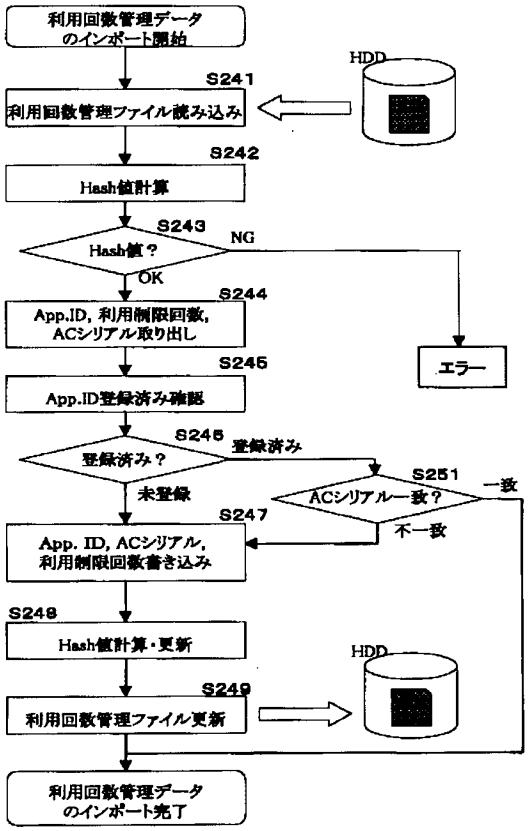
【図３８】


SP管理領域
SP#1管理領域
SP#1,User001
App.ID#1, AC Serial#1, Count#1
App.ID#2, AC Serial#2, Count#2
SP#1,User002
App.ID#1, AC Serial#5, Count#2
App.ID#3, AC Serial#3, Count#5
SP#2管理領域
SP#2,User001
App.ID#5, AC Serial#8, Count#1
App.ID#6, AC Serial#6, Count#2
SP#2,User003
App.ID#6, AC Serial#11, Count#2
App.ID#7, AC Serial#12, Count#3

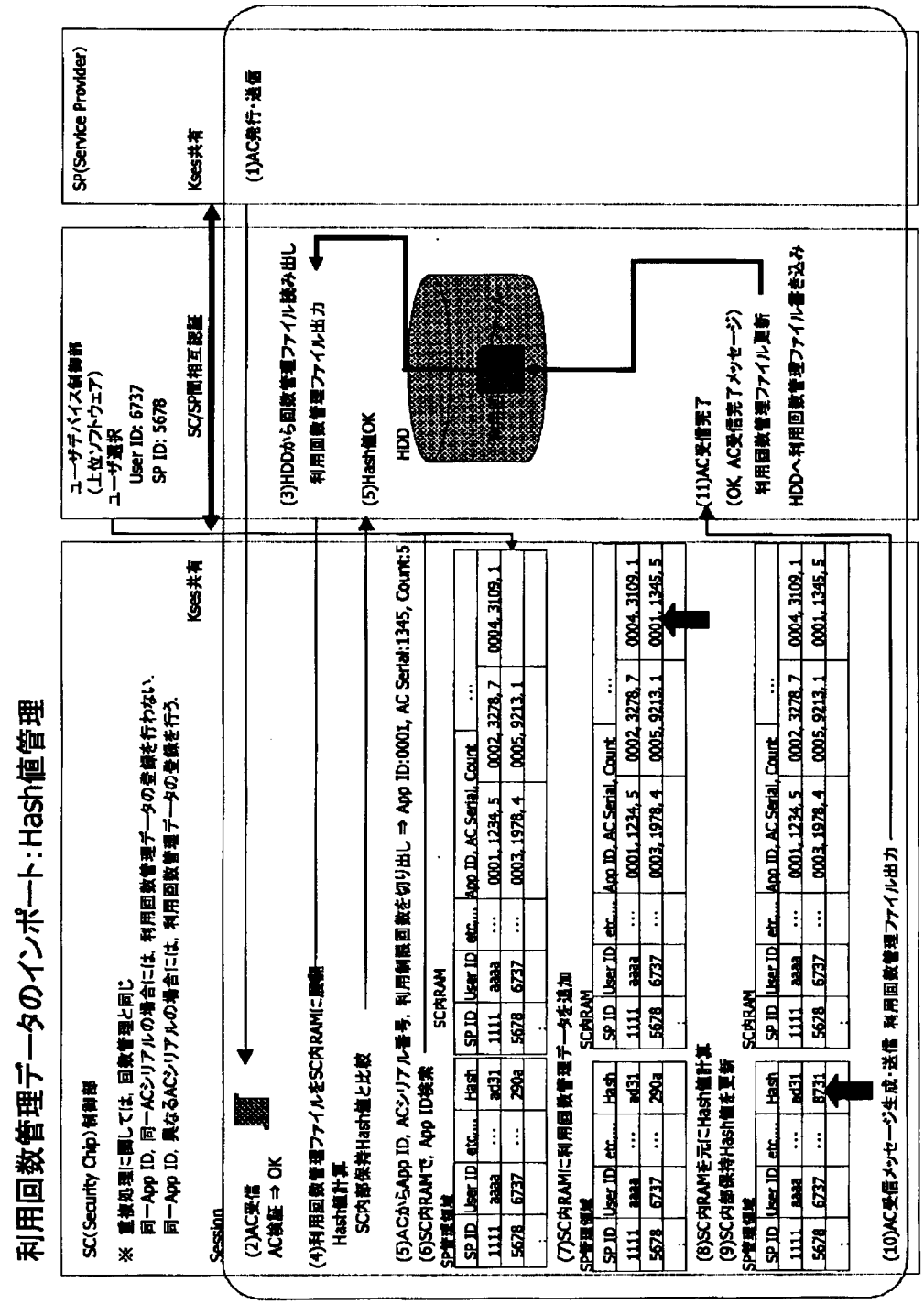
【図３９】


利用回数管理データのインポート処理開始
S221
属性証明書から アプリケーションID、 利用制限回数、 属性証明書シリアル番号、 取り出し
S222
アプリケーションID 登録済み確認処理
S223
登録済み？
登録済み
未登録
S224
ACシリアル一致？
一致
不一致
S225
AppID、ACシリアル、 利用制限回数、書き込み
回数情報 インポート処理終了

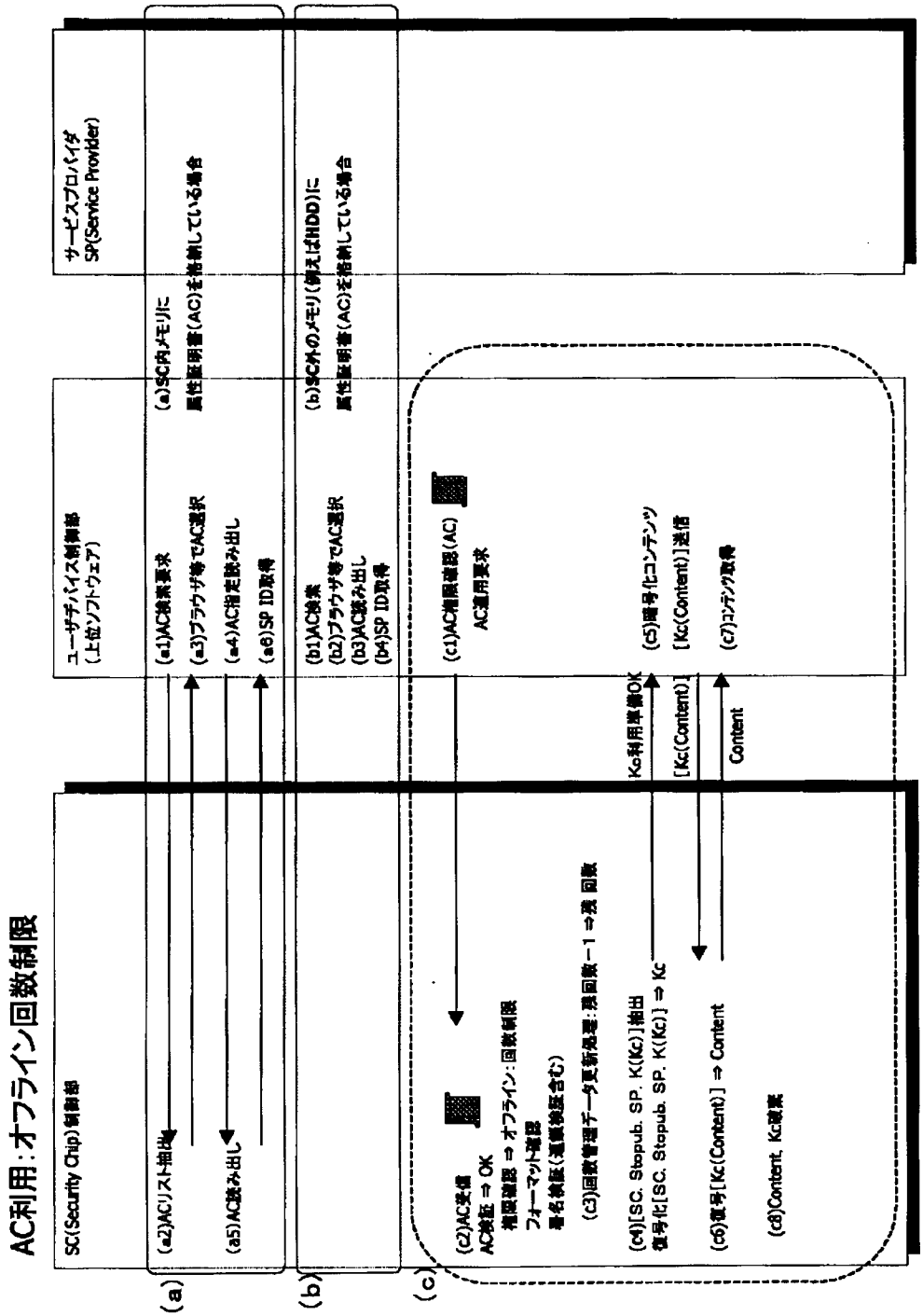
【図４１】


利用回数管理データのインポート開始
HDD
S241
利用回数管理ファイル読み込み
S242
Hash値計算
S243
Hash値？
NG
OK
エラー
S244
App.ID, 利用制限回数, ACシリアル取り出し
S245
App.ID登録済み確認
S246
登録済み？
登録済み
未登録
S251
ACシリアル一致？
一致
不一致
S247
App. ID, ACシリアル, 利用制限回数書き込み
S248
Hash値計算・更新
HDD
S249
利用回数管理ファイル更新
利用回数管理データのインポート完了

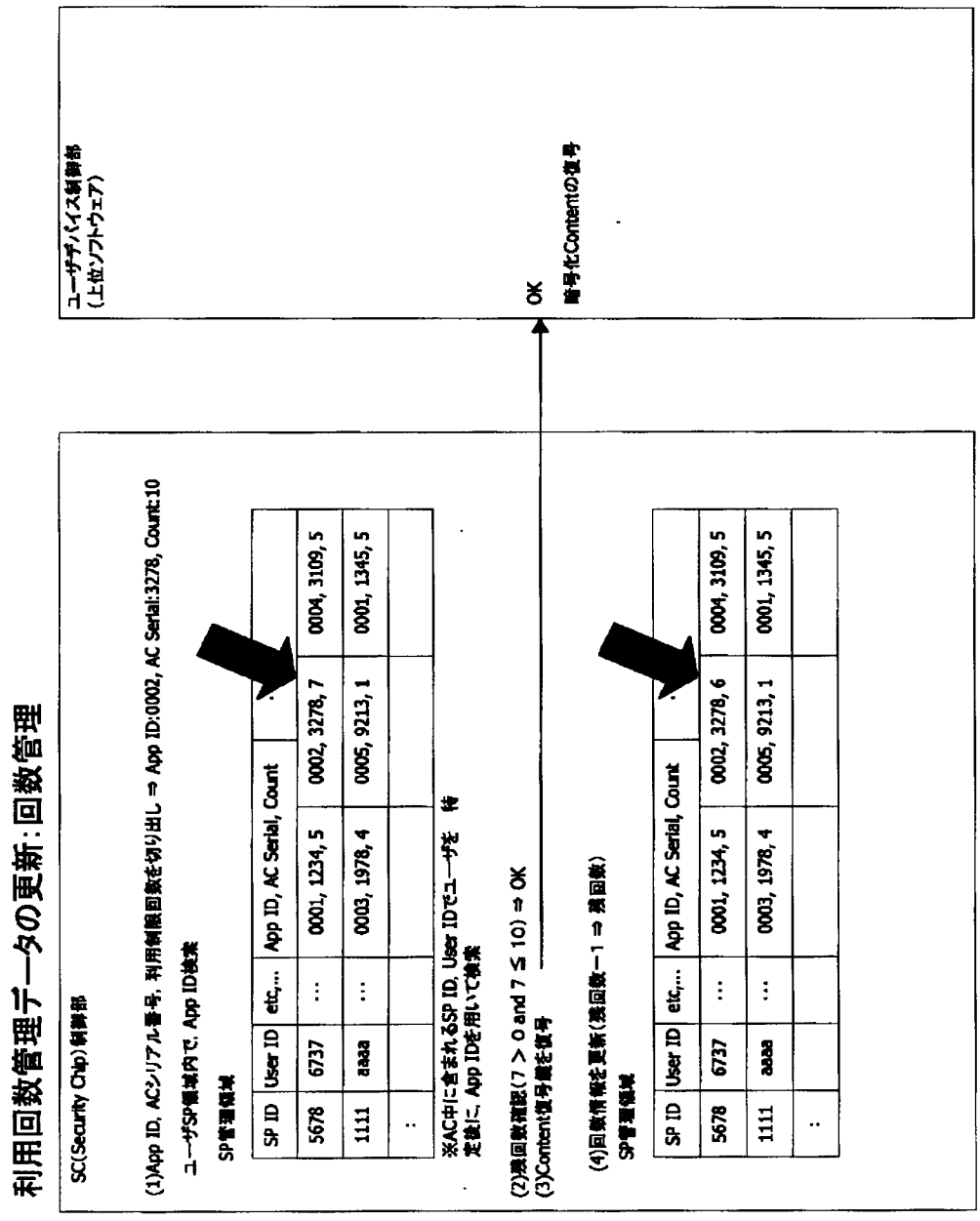
【図４０】


利用回数管理データのインポート：Hash値管理
SC(Security Chip)制御部
※ 重複処理に関しては、回数管理と同じ
同一App ID, 同一ACシリアルの場合には、利用回数管理データの登録を行わない。
同一App ID, 異なるACシリアルの場合には、利用回数管理データの登録を行う。
Session
Kses共有
(2)AC受信
AC検証 ⇒ OK
(4)利用回数管理ファイルをSC内RAMに展開
Hash値計算
SC内部保持Hash値と比較
(5)ACからApp ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0001, AC Serial:1345, Count:5
(6)SC内RAMで, App ID検索
SC内RAM
SP管理領域
SP ID User ID etc..... Hash
1111 aaaa ... ad31
5678 6737 ... 290a
SP ID User ID etc.... App ID, AC Serial, Count ...
1111 aaaa ... 0001, 1234, 5 0002, 3278, 7 0004, 3109, 1
5678 6737 ... 0003, 1978, 4 0005, 9213, 1
(7)SC内RAMに利用回数管理データを追加
SC内RAM
SP管理領域
SP ID User ID etc..... Hash
1111 aaaa ... ad31
5678 6737 ... 290a
SP ID User ID etc.... App ID, AC Serial, Count ...
1111 aaaa ... 0001, 1234, 5 0002, 3278, 7 0004, 3109, 1
5678 6737 ... 0003, 1978, 4 0005, 9213, 1 0001, 1345, 5
(8)SC内RAMを元にHash値計算
(9)SC内部保持Hash値を更新
SC内RAM
SP管理領域
SP ID User ID etc..... Hash
1111 aaaa ... ad31
5678 6737 ... 6731
SP ID User ID etc.... App ID, AC Serial, Count ...
1111 aaaa ... 0001, 1234, 5 0002, 3278, 7 0004, 3109, 1
5678 6737 ... 0003, 1978, 4 0005, 9213, 1 0001, 1345, 5
(10)AC受信メッセージ生成・送信 利用回数管理ファイル出力
Kses共有
SC/SP間相互認証
SP(Service Provider)
(1)AC発行・送信
ユーザデバイス制御部
(上位ソフトウェア)
ユーザ選択
User ID: 6737
SP ID: 5678
(3)HDDから回数管理ファイル読み出し
利用回数管理ファイル出力
(5)Hash値OK
HDD
(11)AC受信完了
(OK, AC受信完了メッセージ)
利用回数管理ファイル更新
HDDへ利用回数管理ファイル書き込み

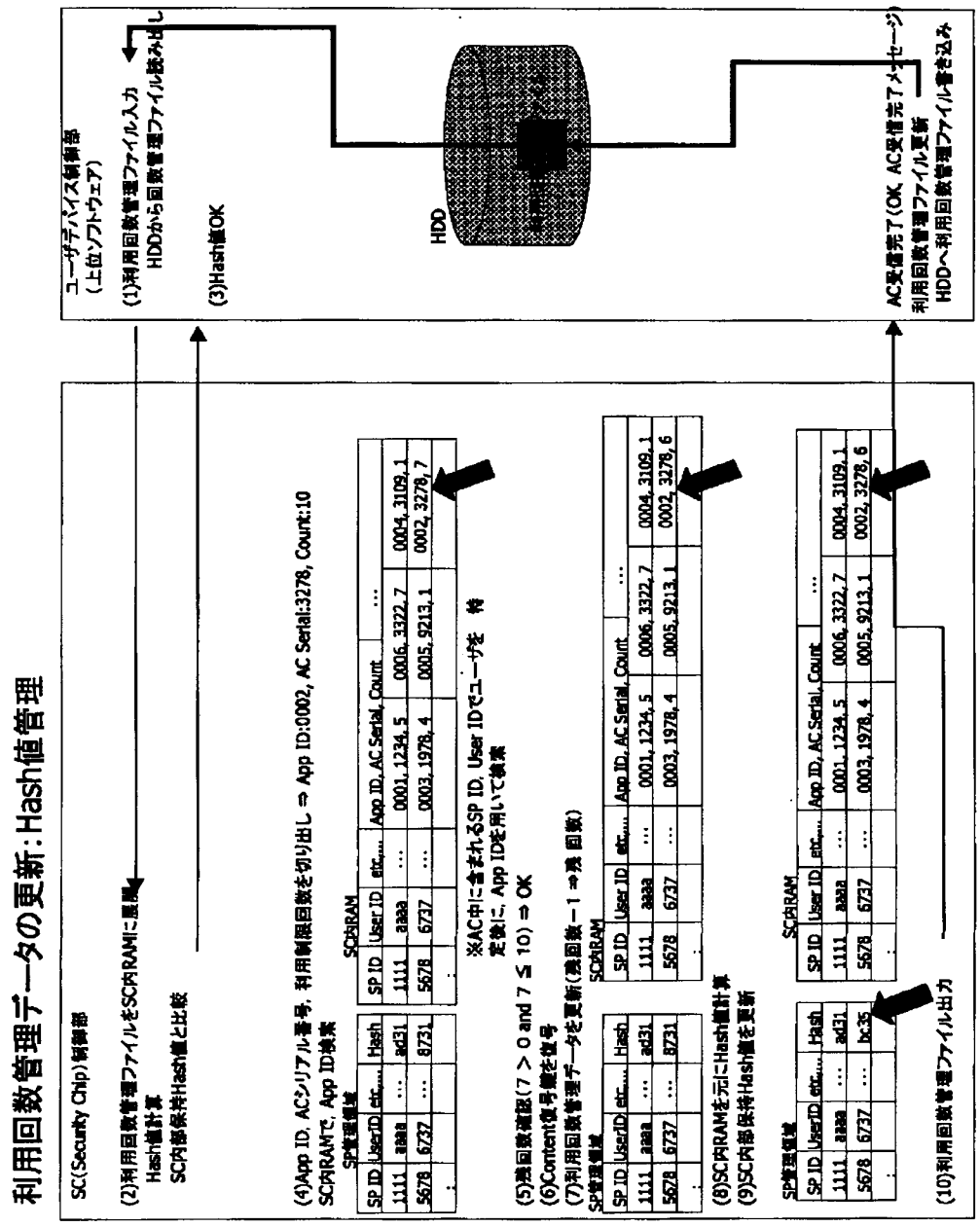
【図４２】


AC利用：オフライン回数制限
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内メモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)AC権限確認(AC)
AC利用要求
(c2)AC受領
AC検証 ⇒ OK
権限確認 ⇒ オフライン：回数制限
フォーマット確認
署名検証(証明書検証含む)
(c3)回数管理データ更新処理：残回数－1 ⇒残 回数
(c4)[SC. Stopub. SP. K(Kc)]抽出
復号化[SC. Stopub. SP. K(Kc)] ⇒ Kc
(c5)暗号化コンテンツ
[Kc(Content)]送信
(c6)復号[Kc(Content)] ⇒ Content
(c7)コンテンツ取得
(c8)Content, Kc破棄
Kc利用準備OK
[Kc(Content)]
Content

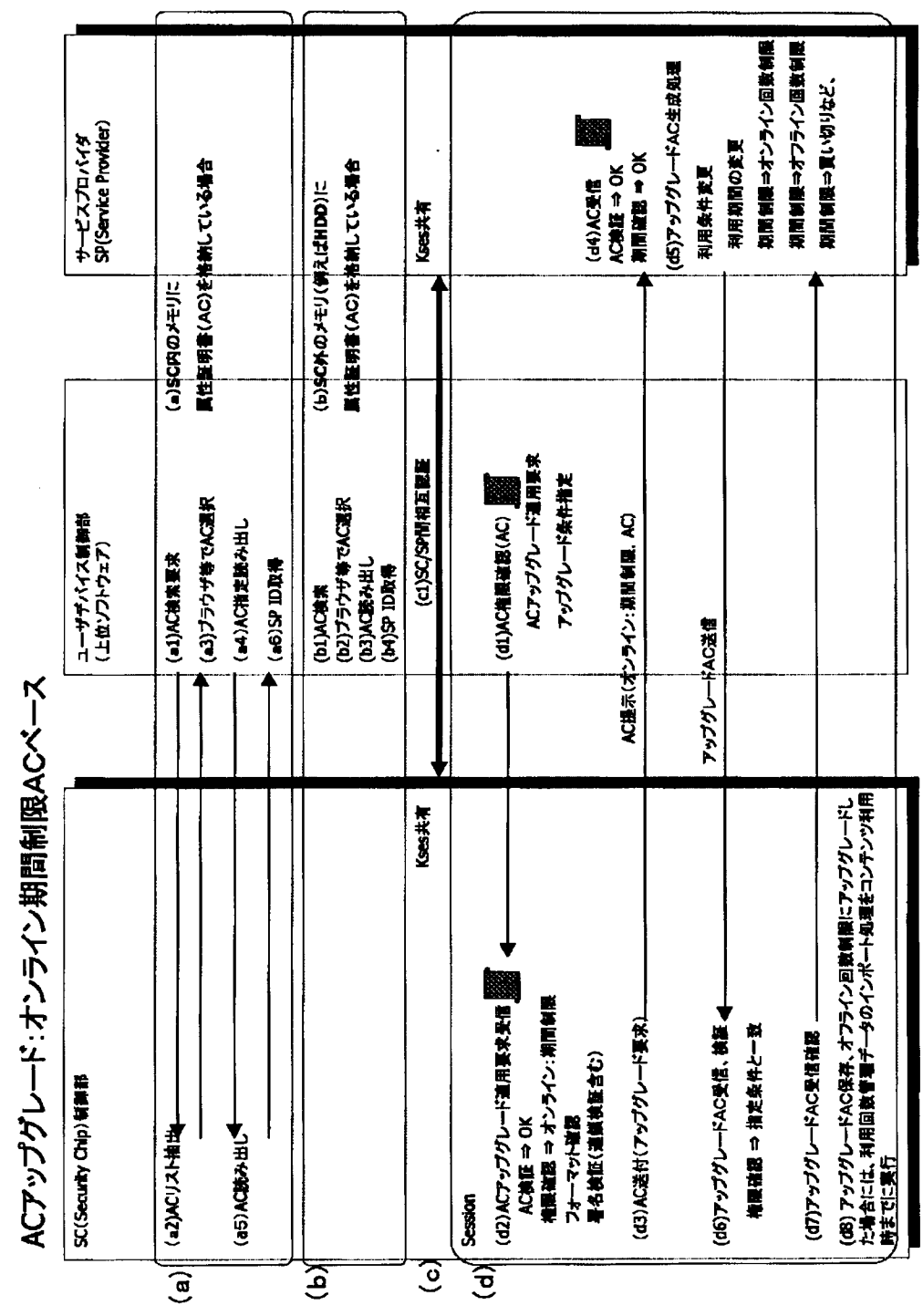
【図４３】


利用回数管理データの更新：回数管理
SC(Security Chip)制御部
(1)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0002, AC Serial:3278, Count:10
ユーザSP領域内で, App IDを検索
SP管理領域
SP ID
User ID
etc,...
App ID, AC Serial, Count
5678
6737
…
0001, 1234, 5
0002, 3278, 7
0004, 3109, 5
1111
aaaa
…
0003, 1978, 4
0005, 9213, 1
0001, 1345, 5
※ACに含まれるSP ID, User IDでユーザを 特定し, App IDを用いて検索
(2)残回数確認(7 > 0 and 7 ≦ 10) ⇒ OK
(3)Content復号鍵を復号
(4)回数情報を更新(残回数−1 ⇒ 残回数)
SP管理領域
0002, 3278, 6
0004, 3109, 5
0003, 1978, 4
0005, 9213, 1
0001, 1345, 5
ユーザデバイス制御部
(上位ソフトウェア)
OK
暗号化Contentの復号

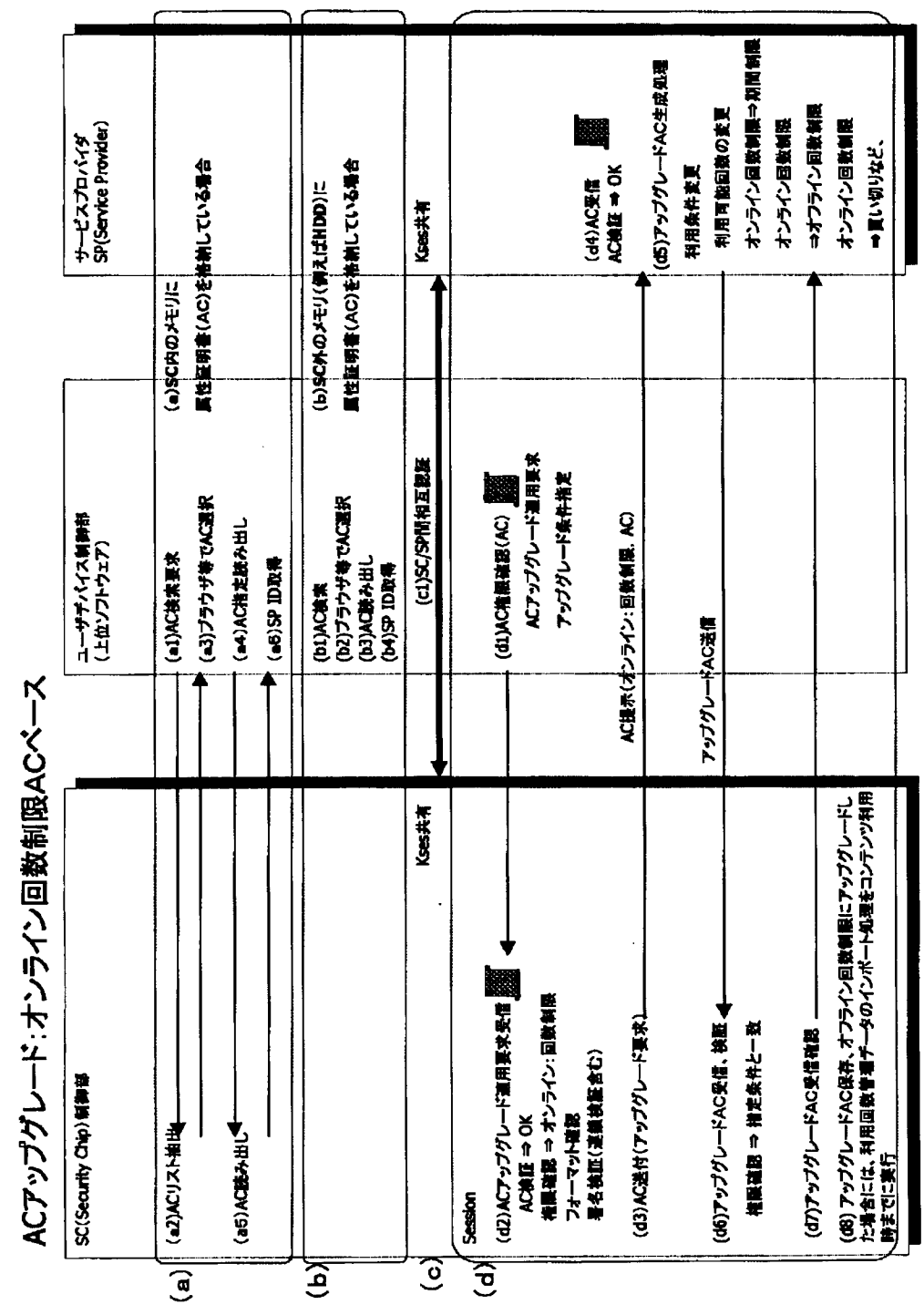
【図４４】


利用回数管理データの更新:Hash値管理
SC(Security Chip)制御部
(2)利用回数管理ファイルをSC内RAMに展開
Hash値計算
SC内部保持Hash値と比較
(4)App ID, ACシリアル番号, 利用制限回数を切り出し ⇒ App ID:0002, AC Serial:3278, Count:10
SC内RAMで, App ID検索
SP管理領域
SC内RAM
SP ID
UserID
etc....
Hash
App ID, AC Serial, Count
1111 aaaa ... ad31 0001, 1234, 5 0006, 3322, 7 0004, 3109, 1
5678 6737 ... 8731 0003, 1978, 4 0005, 9213, 1 0002, 3278, 7
※AC中に含まれるSP ID, User IDでユーザを 特
定後に, App IDを用いて検索
(5)残回数減算(7 > 0 and 7 ≤ 10) ⇒ OK
(6)Content復号鍵を復号
(7)利用回数管理データを更新(残回数－1 ⇒残 回数)
(8)SC内RAMを元にHash値計算
(9)SC内部保持Hash値を更新
5678 6737 ... bc35
(10)利用回数管理ファイル出力
ユーザデバイス制御部
(上位ソフトウェア)
(1)利用回数管理ファイル入力
HDDから回数管理ファイル読み出し
(3)Hash値OK
HDD
AC受信完了(OK, AC受信完了メッセージ)
利用回数管理ファイル更新
HDDへ利用回数管理ファイル書き込み

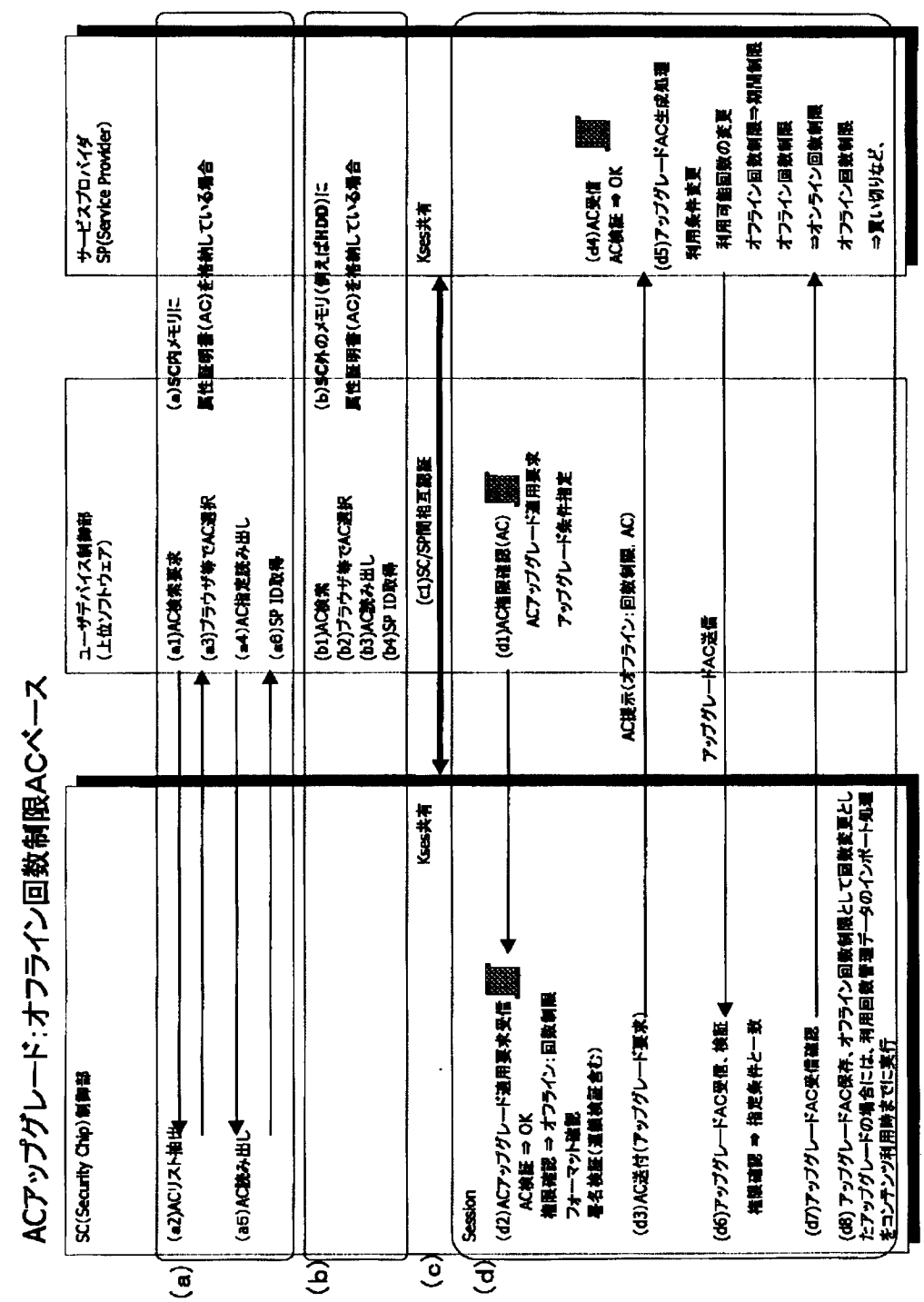
【図４５】


ACアップグレード:オンライン期間制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
(a4)AC属性読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内のメモリに
属性証明書(AC)を格納している場合
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード運用要求
アップグレード条件指定
(d2)ACアップグレード運用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:期間制限
フォーマット確認
署名検証(連鎖検証含む)
(d3)AC送付(アップグレード要求)
AC提示(オンライン:期間制限, AC)
(d4)AC受信
AC検証 ⇒ OK
期間確認 ⇒ OK
(d5)アップグレードAC生成処理
利用条件変更
利用期間の変更
期間制限⇒オンライン回数制限
期間制限⇒オフライン回数制限
期間制限⇒置い切りなど、
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
アップグレードAC送信
(d7)アップグレードAC受信確認
(d8) アップグレードAC保存、オフライン回数制限にアップグレードした場合には、利用回数管理データのインポート処理をコンテンツ利用時までに実行

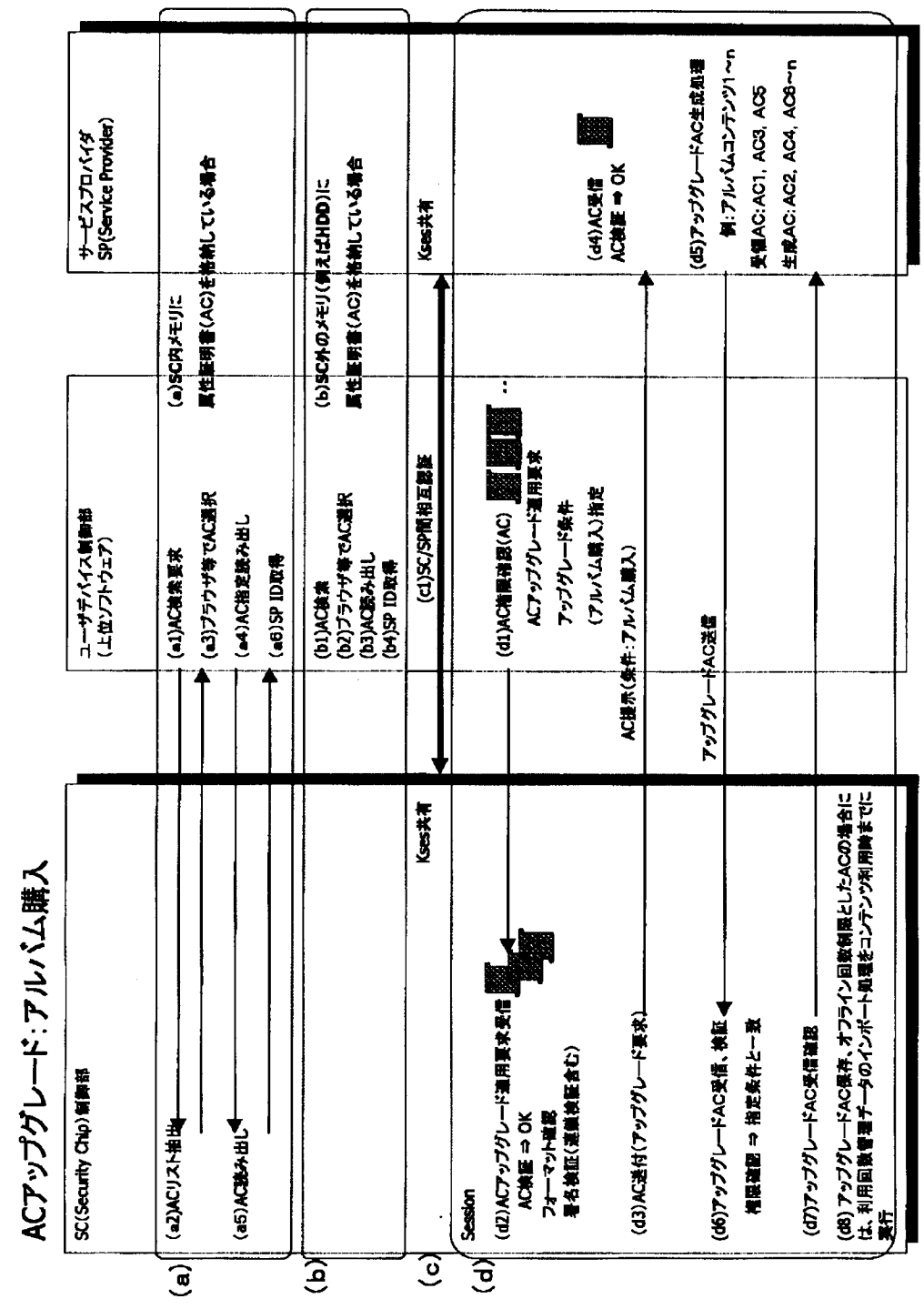
【図４６】


ACアップグレード:オンライン回数制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(a1)AC検索要求
(a)SC内のメモリに
(a3)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a2)ACリスト抽出
(b)
(b1)AC検索
(b)SC外のメモリ(例えばHDD)に
(b2)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(b3)AC読み出し
(b4)SP ID取得
(c)
(c1)SC/SP間相互認証
Kses共有
(d)
Session
(d1)AC権限確認(AC)
ACアップグレード運用要求
アップグレード条件指定
(d2)ACアップグレード運用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オンライン:回数制限
フォーマット確認
署名検証(連鎖検証含む)
(d4)AC受信
AC検証 ⇒ OK
AC提示(オンライン:回数制限, AC)
(d3)AC送付(アップグレード要求)
(d5)アップグレードAC生成処理
利用条件変更
利用可能回数の変更
オンライン回数制限⇒期間制限
オンライン回数制限
⇒オフライン回数制限
オンライン回数制限
⇒買い切りなど、
アップグレードAC送信
(d6)アップグレードAC受信, 検証
権限確認 ⇒ 指定条件と一致
(d7)アップグレードAC受信確認
(d8) アップグレードAC提供, オフライン回数制限にアップグレードした場合には, 利用回数管理データのインポート処理をコンテンツ利用時までに実行
Kses共有

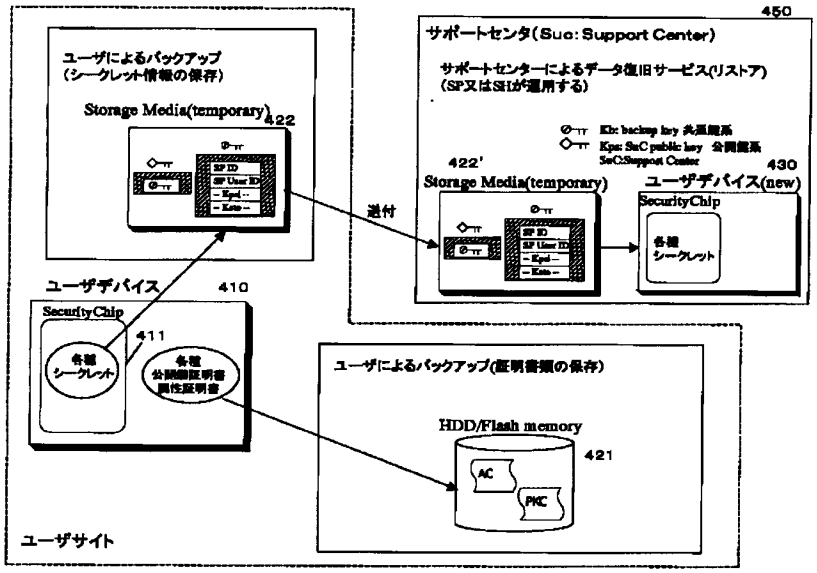
【図４７】


ACアップグレード:オフライン回数制限ACベース
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)AC検索要求
(a)SC内メモリに
(a2)ACリスト抽出
(a3)ブラウザ等でAC選択
属性証明書(AC)を格納している場合
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(b1)AC検索
(b)SC外のメモリ(例えばHDD)に
(b2)ブラウザ等でAC選択
(b3)AC読み出し
属性証明書(AC)を格納している場合
(b4)SP ID取得
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC情報確認(AC)
ACアップグレード運用要求
アップグレード条件指定
(d2)ACアップグレード運用要求受信
AC検証 ⇒ OK
権限確認 ⇒ オフライン:回数制限
フォーマット確認
署名検証(連鎖検証含む)
(d4)AC受信
AC検証 ⇒ OK
AC提示(オフライン:回数制限, AC)
(d3)AC送付(アップグレード要求)
(d5)アップグレードAC生成処理
利用条件変更
利用可能回数の変更
オフライン回数制限⇒期間制限
オフライン回数制限
⇒オンライン回数制限
アップグレードAC送信
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
オフライン回数制限
⇒オンライン回数制限
(d7)アップグレードAC受信確認
(d8) アップグレードAC保存、オフライン回数制限として回数変更とした
アップグレードの場合には、利用回数管理データのインポート処理
をコンテンツ利用時までに実行

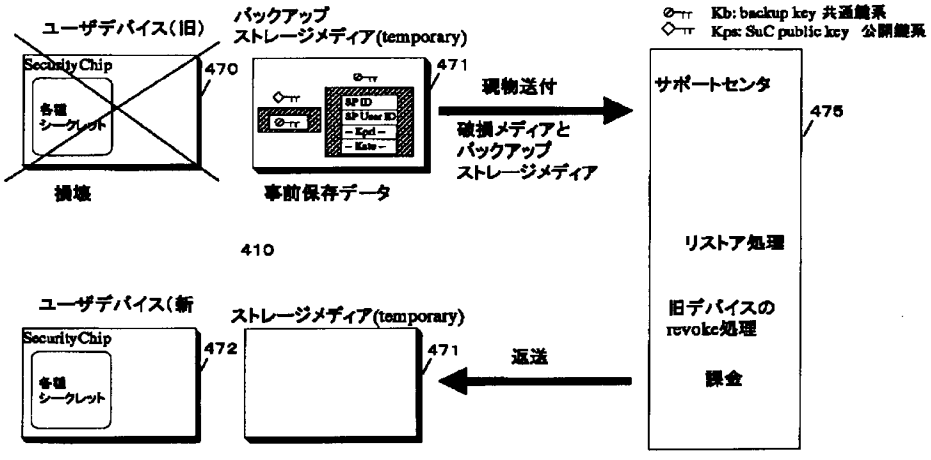
【図４８】


ACアップグレード：アルバム購入
SC(Security Chip)制御部
ユーザデバイス制御部
(上位ソフトウェア)
サービスプロバイダ
SP(Service Provider)
(a)
(b)
(c)
(d)
(a1)ACリスト要求
(a2)ACリスト提出
(a3)ブラウザ等でAC選択
(a4)AC指定読み出し
(a5)AC読み出し
(a6)SP ID取得
(a)SC内メモリに
属性証明書(AC)を格納している場合
(b1)AC検索
(b2)ブラウザ等でAC選択
(b3)AC読み出し
(b4)SP ID取得
(b)SC外のメモリ(例えばHDD)に
属性証明書(AC)を格納している場合
(c1)SC/SP間相互認証
Kses共有
Kses共有
Session
(d1)AC権限確認(AC)
ACアップグレード運用要求
アップグレード条件
(アルバム購入)指定
(d2)ACアップグレード運用要求受信
AC検証 ⇒ OK
フォーマット確認
署名検証(運用検証含む)
(d3)AC送付(アップグレード要求)
AC提示(条件:アルバム購入)
(d4)AC受信
AC検証 ⇒ OK
(d5)アップグレードAC生成処理
例:アルバムコンテンツ1～n
受領AC:AC1, AC3, AC5
生成AC:AC2, AC4, AC6～n
アップグレードAC送信
(d6)アップグレードAC受信、検証
権限確認 ⇒ 指定条件と一致
(d7)アップグレードAC受信確認
(d8)アップグレードAC展示、オフライン回数制限としたACの場合には、利用回数管理データのインポート処理をコンテンツ利用時までに実行

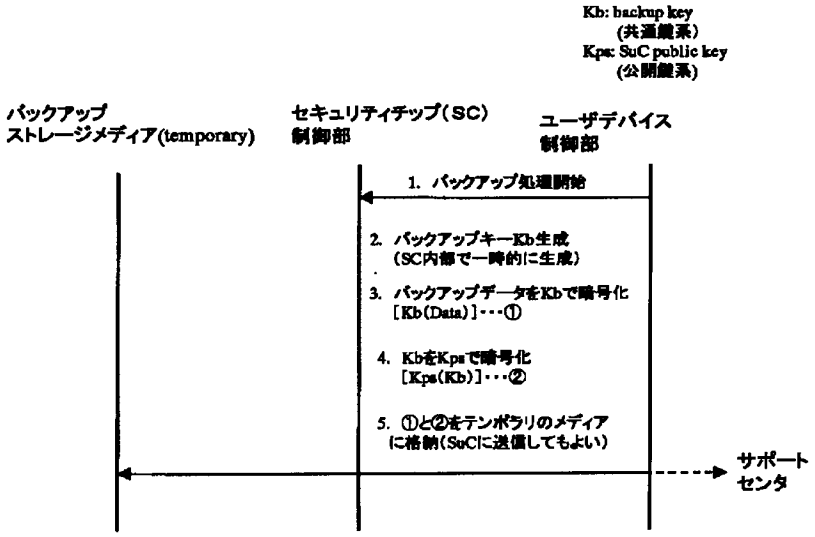
【図４９】


450
サポートセンタ(Suc: Support Center)
サポートセンターによるデータ復旧サービス(リストア)
(SP又はSHが運用する)
Kb: backup key 共通鍵系
Kps: SuC public key 公開鍵系
SuC:Support Center
430
ユーザによるバックアップ
(シークレット情報の保存)
Storage Media(temporary)
422
422'
Storage Media(temporary)
ユーザデバイス(new)
SecurityChip
各種
シークレット
送付
ユーザデバイス
410
SecurityChip
411
各種
シークレット
各種
公開鍵証明書
属性証明書
ユーザによるバックアップ(証明書類の保存)
HDD/Flash memory
421
AC
PKC
ユーザサイト

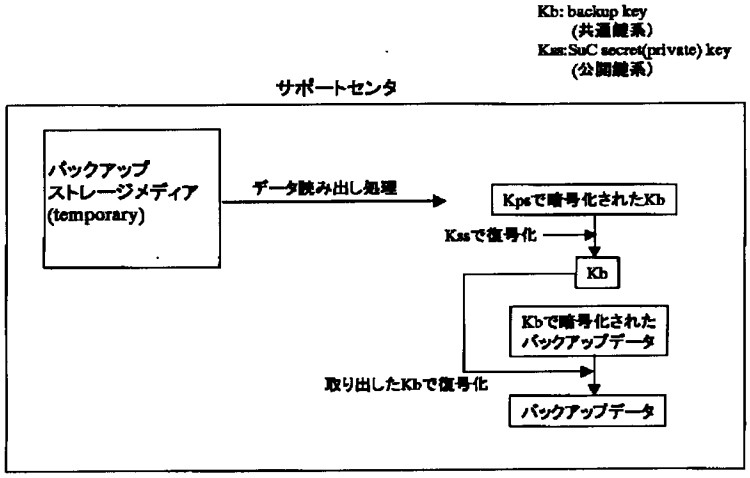
【図５０】


Kb: backup key 共通鍵系
Kps: SuC public key 公開鍵系
ユーザデバイス(旧)
バックアップ
ストレージメディア(temporary)
SecurityChip
470
各種
シークレット
471
現物送付
破損メディアと
バックアップ
ストレージメディア
サポートセンタ
475
損壊
事前保存データ
リストア処理
410
旧デバイスの
revoke処理
ユーザデバイス(新
ストレージメディア(temporary)
SecurityChip
472
各種
シークレット
471
返送
課金

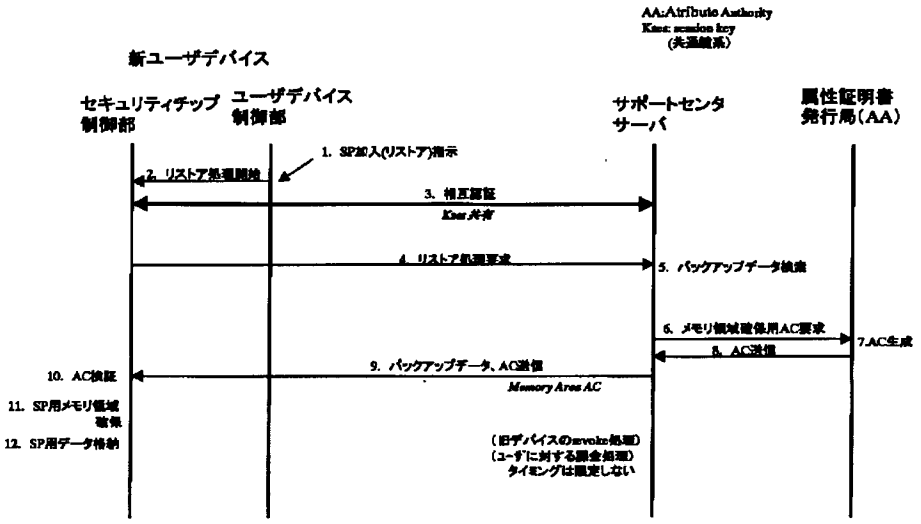
【図５１】


Kb: backup key
(共通鍵系)
Kps: SuC public key
(公開鍵系)
バックアップ
ストレージメディア(temporary)
セキュリティチップ(SC)
制御部
ユーザデバイス
制御部
1. バックアップ処理開始
2. バックアップキーKb生成
(SC内部で一時的に生成)
3. バックアップデータをKbで暗号化
[Kb(Data)]・・・①
4. KbをKpsで暗号化
[Kps(Kb)]・・・②
5. ①と②をテンポラリのメディア
に格納(SuCに送信してもよい)
サポート
センタ

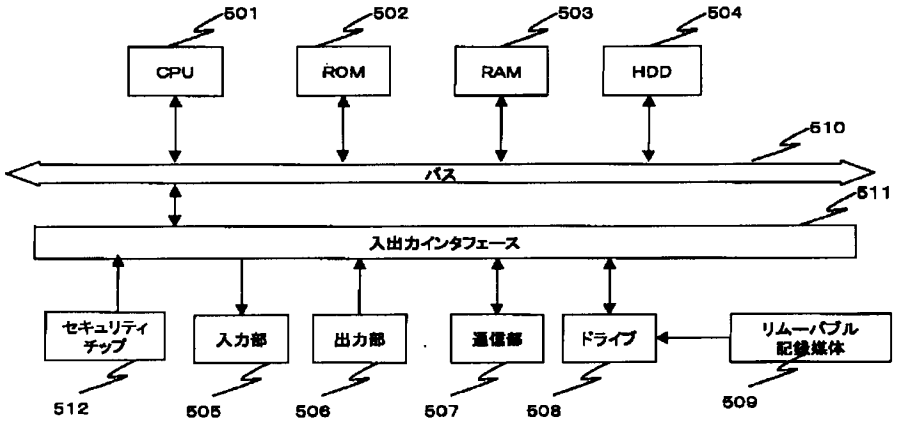
【図５２】


Kb: backup key
(共通鍵系)
Kss:SuC secret(private) key
(公開鍵系)
サポートセンタ
バックアップ
ストレージメディア
(temporary)
データ読み出し処理
Kpsで暗号化されたKb
Kssで復号化
Kb
Kbで暗号化された
バックアップデータ
取り出したKbで復号化
バックアップデータ

【図５３】



【図５４】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
		H04N 7/167	Z

(72)発明者　阿部　博
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　島田　昇
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　江成　正彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　吉野　賢治
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5C064 BA07 BB02 BC06 BC16 BC20
BC23 BD08 BD09
5J104 AA07 AA09 AA16 EA01 EA05
EA06 EA18 KA02 KA06 MA05
NA02 NA03 NA12 NA35 NA36
NA37 NA42 PA05 PA07